НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2019 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі

Виконала: студентка 2 курсу, групи ФБ-71мн
(шифр групи)

Гончаренко Євгенія Олександрівна _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доцент кафедри ІБ Коломицев М.В _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н., доцент кафедри ТК Корнага Я.І. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-науковою програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи, технології та математичні методи кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

_____
(прізвище, ім'я, по батькові)

1. Тема дисертації _____
_____
_____ ,
науковий керівник дисертації _____ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» квітня 2019 р. № 1023-с

2. Термін подання студентом дисертації 06.05.2019 р.

3. Об'єкт дослідження _____
_____

4. Предмет дослідження _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Представлена робота обсягом 92 сторінки містить 12 ілюстрацій, 17 таблиць та 10 джерел за переліком посилань.

Актуальність роботи зумовлюється тим, що в ній висвітлюються проблеми підприємств роздрібної торгівлі, які займають вагому нішу в індустрії як України, так і у всьому світі. Підприємства роздрібної торгівлі, першими впроваджують інноваційні рішення, отримують безсумнівні конкурентні переваги, але при цьому нові технології вимагають нових підходів до СУІБ, яка базується на управлінні ризиками.

Метою даної роботи є підвищення ефективності засобів захисту інформаційних систем підприємств роздрібної торгівлі, шляхом ранньої ідентифікації можливих ризиків інформаційної безпеки з урахуванням особливостей даної індустрії.

Об’єктом дослідження є інформаційна безпека підприємств роздрібної торгівлі.

Предмет досліджень – методи і підходи до оцінки ризиків інформаційної безпеки підприємств роздрібної торгівлі.

Методами дослідження було обрано: опрацювання літератури за даною темою, аналіз документації міжнародних стандартів та їх порівняння.

Практичне значення результатів роботи випливає з можливості використання даного підходу для побудови системи управління інформаційною безпекою, яка базується на процесі управління ризиками інформаційної безпеки, а також на основі використання даного підходу для оцінки ризиків інформаційної безпеки реального підприємства провести обробку ризиків для зменшення їх до прийнятного рівня.

Ключові слова: інформаційна безпека, оцінка ризиків, роздрібна торгівля, вразливість, загроза, збитки.

ABSTRACT

This work of 92 pages contains 12 illustrations, 16 tables and 10 literature references.

The relevance of the work is because it covers the problems of retail enterprises, which occupy a significant place in the industry of Ukraine and throughout the world. Retail companies that are the first to implement innovative solutions, they receive competitive advantages, but new technologies require new approaches to information security management system, that based on risk management.

The purpose of this work is to increase the effectiveness of means of protecting information systems of retailers by early identification of possible information security risks, taking into account the characteristics of this industry.

The object of research is the information security of retail enterprises.

As a subject of research deals with retailer information security risks.

When writing the work theoretical analysis and synthesis of scientific literature, documentation of international standards was carried out.

The value of the work results is to use this approach to build an information security management system, which is based on the information security risk management process, and based on the results of using the proposed approach for a real retailer to process risks to reduce them to an acceptable level.

Keywords: information security, risk assessment, retail, vulnerability, threat, damage.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PricewaterhouseCoopers (PwC) - міжнародна мережа компаній, що пропонують послуги в області консалтингу та аудиту.

POS-термінал — це електронний пристрій, що зчитує дані пластикової картки з магнітної смуги або чипу, розташованого на пластиковій картці, і зв’язується з банком по електронних каналах зв’язку.

Аналіз ризику – систематичне використання інформації про ризик для ідентифікації його джерел і оцінки його величини. Інформація може включати історичні дані про ризик, дані про місця зберігання, думки співробітників про цінності активів і ін.

Доступність – властивість інформації, що полягає в наявності інформації для користувача, коли це необхідно.

Уникнення ризику – рішення не брати участь в ситуації, пов’язаної з ризиком, або відмова від виконання дії, яка може привести до реалізації ризику.

Ідентифікація ризику – процес, спрямований на знаходження і опис елементів ризику (вразливостей, загроз, ймовірності та збитку).

Загроза – умисна дія або випадкова подія, яка може статися з певною ймовірністю, і завдати шкоди організації.

Збиток – негативні наслідки для організації, пов’язані з реалізацією ризику. Можуть включати: фінансові втрати, зниження репутації і лояльності співробітників, несприятливі організаційні зміни і інші наслідки.

Інформаційна безпека (ІБ) – комплекс процесів, дій і документів щодо забезпечення конфіденційності, цілісності та доступності інформації.

Інформаційний актив – будь-яка інформація, яка має цінність для організації.

Конфіденційність – властивість інформації, що полягає в недоступності інформації або не розкриті її змісту неавторизованим особам.

Місце зберігання і обробки інформаційних активів – контейнер, за допомогою якого збирається, передається, обробляється і зберігається інформація. Прикладами місць зберігання можуть бути: документ в паперовому та електронному вигляді, інформаційна система, канали передачі даних, приміщення, людина та ін.

Модель загроз ІБ – опис існуючих загроз ІБ, можливостей і наслідків для організації в разі їх реалізації.

Залишковий ризик – ризик, який залишається після обробки початкового оціненого ризику.

Оцінка ризику – процес порівняння оціночної величини ризику до встановлених критеріїв ризику для визначення рівня значущості ризику і подальших дій по його обробці.

Обробка ризику – процес вибору і реалізації заходів щодо модифікації ризику, що може включати дії щодо зниження, уникнення, передачі і прийняття ризику.

Передача ризику – передача частини відповідальності за управління ризиком третій стороні (страхової компанії або компанії, яка займається аутсорсингом процесів і послуг).

ПЗ – програмне забезпечення.

Прийняття ризику – згода компанії понести можливі збитки від реалізації ризику, пов’язаного з певною діяльністю.

Ризик-апетит – рівень ризику, на який готова піти організація для досягнення бізнес-цілей; являє собою баланс між потенційними вигодами від виконання бізнес-діяльності і збитку, до якого дані дії можуть привести.

Ризик інформаційної безпеки (ІБ) – рівень збитку, який понесе компанія, в разі реалізації загрози з використанням уразливості місця зберігання і обробки інформації компанії.

Система управління інформаційною безпекою (СУІБ) – система управління, призначена для створення, впровадження, експлуатації, моніторингу, аналізу, супроводу і вдосконалення ІБ.

Управління ризиком – скоординовані дії організації з контролю за ризиками ІБ, що включає їх ідентифікацію, оцінку і обробку.

Уразливість – відсутність або неефективність контролю ІБ щодо захисту інформації в місці зберігання і обробки від порушення її конфіденційності, цілісності і доступності.

Цілісність – властивість інформації, що полягає в забезпеченні її точності і повноти.

ВСТУП

У сучасному світі все більше уваги приділяється захисту інформації. Як і в будь-якому іншому виді діяльності, грамотне планування забезпечення безпеки інформації є найважливішим етапом на шляху до забезпечення безпеки даних.

Організація ефективної системи захисту інформації стає критично важливим стратегічним чинником розвитку будь-якого підприємства, так як, інформація є одним з ключових елементів бізнесу. При цьому під інформацією розуміються не тільки статичні інформаційні ресурси (бази даних, поточні налаштування обладнання та інші), а й динамічні інформаційні процеси обробки даних.

Інформаційна безпека підприємства - це стан захищеності інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Для створення надійної системи управління інформаційною безпекою (СУІБ) необхідно виробити політику ІБ, провести аналіз ризиків, скласти план заходів щодо забезпечення ІБ, вибрати програмні, технічні та програмно-технічні засоби забезпечення ІБ.

Оскільки на основі даних отриманих в ході аналізу захищеності підприємства будується вся система захисту інформації, етап аналізу ризиків є одним з основних, а також одним з найскладніших етапів побудови СУІБ, так як вимагає чималих ресурсів (людських, матеріальних, часових).

Сьогодні аналізу ризиків інформаційної безпеки приділяється все більше уваги. Цьому є кілька основних причин: невпинний ріст використання інформаційних технологій в процесі діяльності практично будь-якого сучасного підприємства, збільшення цінності інформації, що обробляється і генерується в процесі роботи підприємств, а також інтеграція різних інформаційних продуктів з метою покриття всіх потреб підприємства.

Роздрібна торгівля невпинно зростає та удосконалюється, використовуючи для бізнесу різноманітні інновації. Це ще більше ускладнює

проблему надійного захисту інформації, призводить до того, що нині інформаційна безпека стає ключовим фактором, що забезпечує довіру споживачів та збереження конкурентоспроможності.

Актуальність роботи зумовлюється тим, що в ній висвітлюються проблеми підприємств роздрібної торгівлі, які займають вагому нішу в індустрії як України, так і у всьому світі. Підприємства роздрібної торгівлі першими впроваджують інноваційні рішення, отримують безсумнівні конкурентні переваги, але при цьому не можна забувати і про те, що нові технології вимагають нових підходів до СУІБ, яка базується на управлінні ризиками.

Метою даної роботи є підвищення ефективності засобів захисту інформаційних систем підприємств роздрібної торгівлі, шляхом ранньої ідентифікації можливих ризиків інформаційної безпеки з урахуванням особливостей даної індустрії.

Для досягнення даної мети було поставлено такі завдання:

- Аналіз проблем інформаційної безпеки підприємств роздрібної торгівлі;
- Огляд існуючих методологій та стандартів з управління ризиками інформаційної безпеки, порівняльний аналіз, виявлення недоліків та переваг;
- Визначення релевантного для підприємств роздрібної торгівлі підходу до оцінки ризиків інформаційної безпеки;
- Оцінка ризиків інформаційної безпеки для реального підприємства, що належить до роздрібної торгівлі;
- Визначення місць зберігання та обробки інформації, які мають ризики високого рівня
- Визначення рекомендацій щодо зменшення ризиків високого рівня.

Методами дослідження обрано: опрацювання літератури за даною темою, аналіз документації міжнародних стандартів.

Наукова новизна даної роботи полягає у адаптації методів управління ризиками інформаційної безпеки для визначення оптимального підходу до оцінки ризиків для підприємств роздрібної торгівлі. Визначення такого підходу припускає більш успішну протидію сучасним кібер-зловмисникам, забезпечення безпеки, орієнтованої на захист від загроз шляхом впровадження превентивних засобів захисту.

Практичне значення результатів роботи випливає з можливості використання даного підходу для побудови системи управління інформаційною безпекою, яка базується на процесі управління ризиками інформаційної безпеки, а також на основі використання даного підходу для оцінки ризиків інформаційної безпеки підприємства провести обробку ризиків для зменшення їх до прийнятного рівня.

Таким чином **об’єктом дослідження** є інформаційна безпека підприємств роздрібної торгівлі.

Предмет досліджень – методи і підходи до оцінки ризиків інформаційної безпеки підприємств роздрібної торгівлі.

1 ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ РОЗДРІБНОЇ ТОРГІВЛІ

Роздрібна торгівля у новому тисячолітті – складний та динамічний сектор бізнесу. І це однаковою мірою стосується як високорозвинених країн, так і країн, що розвиваються. Поява нових торговельних мереж і, як наслідок, збільшення конкуренції у сфері роздрібної торгівлі ставлять нові завдання перед підприємствами. У сучасному ритейлі відбуваються стрімкі зміни. Такі основні тренди, як зміна потреб споживачів та їхня дедалі більша зацікавленість не лише у товарах, але й у позитивному досвіді купівлі, консолідація ритейлерів, поява стратегій багатоканальної торгівлі, зміна природи конкуренції як всередині, так і між форматами торгівлі, глобалізація і технологічні прориви впливають на способи ведення ритейл-бізнесу в новому столітті.

За останні роки сегмент роздрібної торгівлі став набирати обертів за кількістю впроваджуваних інформаційних технологій, особливо це стосується частини мобілізації бізнес-процесів. У зв’язку з цим продукти і послуги в області інформаційної безпеки стали для роздрібної торгівлі як ніколи актуальні.

Питання щодо забезпечення безпеки є одним з основоположних у сфері управління підприємством. Зростаюча кількість загроз становить небезпеку не тільки для товарно-матеріальних цінностей, а й для здоров’я і життя людей, а також для самого розвитку бізнесу.

У ритейлі в 2018 році половина кібератак (52%) була спрямована на веб-додатки, переважно онлайн-магазини [4]. В ході таких атак зловмисники компрометували облікові дані клієнтів, викрадали дані їх платіжних карт, порушували роботу веб-додатків. Крім того, майже кожна четверта атака (25%) полягала у впровадженні шкідливого програмного забезпечення [5] (Рисунок 1.1).

З огляду на, що великі підприємства роздрібної торгівлі можуть обробляти тисячі транзакцій щодня через свої POS-термінали і існує процвітаючий ринок для викрадених даних кредитних карт, з цього слідує, що POS-термінали є бажаною ціллю для кіберзлочинців [6].

Рисунок 1.1 – Поширені методи атак на підприємства роздрібної торгівлі

Зростає визнання того, що інформаційна безпека впливає на більш широкий спектр бізнес-ризиків, і програми безпеки більше не є виключною компетенцією департаментів інформаційних технологій. Бажання володіти більш комплексним підходом до безпеки перейшло до самих лідерів бізнесу. Приділяється більше уваги до співробітників, впроваджується перевірки на поліграфах, адже вагома частина атак досі здійснюється внутрішніми зловмисниками (Рисунок 1.2). Не слід випускати з уваги ризики, які несуть треті сторони. У сучасній взаємозалежній бізнес-екосистемі стан безпеки третіх сторін може надати величезний вплив на безпеку підприємств роздрібної торгівлі та створювати нові ризики. У дослідженні PwC [7] повідомляється про 27-відсоткове збільшення числа інцидентів, пов’язаних зі сторонніми постачальниками послуг, підрядниками і діловими партнерами, які часто мають доступ до мережі і даних компанії.

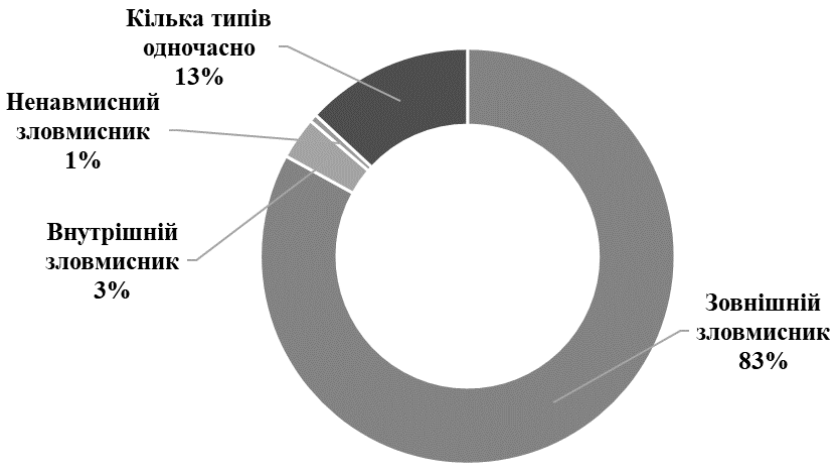

Рисунок 1.2 – Типи зловмисників, що здійснюють атаки на підприємства роздрібної торгівлі

Високий рівень безпеки підприємства галузі роздрібної торгівлі є вагомою конкурентною перевагою і дає змогу значно знизити втрати підприємства від різних загроз. Актуальність питань щодо забезпечення безпеки не підлягає сумніву. Варто враховувати, що тільки комплексний підхід дасть змогу максимально ефективно і мінімальними засобами гарантувати належний рівень безпеки функціонування підприємства.

Система безпеки – це єдиний комплекс організаційних, технічних і управлінських заходів, які тісно взаємопов’язані між собою. Побудова такої системи є унікальним продуктом, який максимально швидко поверне інвестовані кошти і почне приносити прибуток. З огляду на це, існує потреба у впровадженні систем безпеки у роздрібній торгівлі, орієнтованих на сучасний ринок і створених для підвищення прибутку та операційної ефективності діяльності.

Всі підприємства роздрібної торгівлі повинні як мінімум зосередитися на наступних областях, щоб знизити ризик інциденту інформаційної безпека [8]:

- Розробити стратегію інформаційної безпеки, орієнтуючись на те, що повинно бути захищене;

- Визначити пріоритети для захисту, починаючи з оцінки ризиків інформаційної безпеки і аналізу вразливостей;
- Визначення ролей та обов’язків щодо досягнення інформаційної безпеки;
- Впроваджувати навчання співробітників з питань інформаційної безпеки і відповідальності за недотримання вимог інформаційної безпеки;
- Впроваджувати інформаційну безпеку в бізнес;
- Розробити детальний план реагування на інциденти для оперативного вирішення і запобігання будь-яких майбутніх атак.

Висновки до розділу 1

Підприємства роздрібної торгівлі зараз займають велику нішу в індустрії як України, так і у всьому світі. Крім того, галузь роздрібної торгівлі безперервно впроваджує різноманітні інновації. Це ще більше ускладнює проблему надійного захисту, змушуючи визнати, що нині інформаційна безпека стає ключовим фактором, що забезпечує довіру споживачів. Підприємства роздрібної торгівлі, першими впроваджують інноваційні рішення, отримують безсумнівні конкурентні переваги, але при цьому не можна забувати і про те, що нові технології вимагають нових підходів до ІБ.

Необхідний постійний перегляд забезпечення безпеки проти сучасного ландшафту кіберзагроз. Історія інформаційної безпеки показує, що стовідсоткового захисту від зловмисників не існує. Кіберзлочинці активно і з великим успіхом розробляють технології подолання існуючих систем захисту і проникнення в мережу. Опинившись ж всередині мережі, вони приступають до злому внутрішніх ресурсів підприємства та пошуку цінної інформації.

Щоб успішно протидіяти сучасним кіберзлочинцям, необхідно забезпечити безпеку, орієнтовану на захист від загроз протягом усього життєвого циклу атаки - до її початку, в процесі розвитку і після закінчення. Саме для цього необхідним є впровадження процесу управління ризиками інформаційної безпеки.

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ УПРАВЛІННЯ РИЗИКАМИ

2.1 Стандарти, орієнтовані на управління ризиками ІБ

В загальному в світі існує кілька десятків різного роду методик і підходів до оцінки ризиків ІБ, таких як: Austrian IT Security Handbook, AS / NZS4360, BSI 100-3, CRISAM, EBIOS, HB167: 200X, ISF IRAM, CRAMM, ISO 27005, MAGERIT, MARION, MEHARI, NIST SP800-30, OCTAVE, OSSTMMRAV, SOMAP та інші, але частина з них вже застаріла і не розвивається, частина не володіє актуальними перекладами на англійську мову з мови країни походження, що робить складним їх вивчення для широкої аудиторії.

В даній роботі будуть розглянуті саме ті методики, які містять розгорнутий підхід, досить широко відомі в Україні і продовжують розвиватися (або ще не втратили своєї актуальності) і відносно легко доступні.

Вибір тієї чи іншої методики залежить від рівня вимог, що ставить перед собою підприємство до забезпечення безпеки інформації, характеру загроз, що беруться до уваги, і ефективності контрольних заходів щодо захисту інформації.

2.1.1 ДСТУ ISO/IEC 27005:2015

ISO 27005 - це стандарт із серії 2700x, що описує підхід до організації всього процесу з управління ризиками інформаційної безпеки. Представлена в стандарті методика оцінки є класичною і має за недоліки зайву академічність і загальність формулювань. Даний стандарт описує настанови і рекомендується до ознайомлення з метою формування загального уявлення про організацію процесу з управління ризиками ІБ [1].

Що мається на увазі під «ризиком» в даному стандарті: ризик - ефект невизначеності на цілі (ефект - це відхилення від передбачуваного (позитивного і / або негативного). Ризик зазвичай виражається у вигляді

комбінації наслідків події ІБ і відповідної ймовірності її виникнення. Невизначеність - це недостатність (навіть часткова) інформації, пов’язаної з розумінням події або знаннями про подію, її наслідками або можливістю виникнення.

Процес менеджменту ризиків інформаційної безпеки складається з визначення обставин, оцінки ризику, обробки ризику, прийняття ризику, обміну інформацією щодо ризику, а також моніторингу та перегляду ризику (Рисунок 2.1).

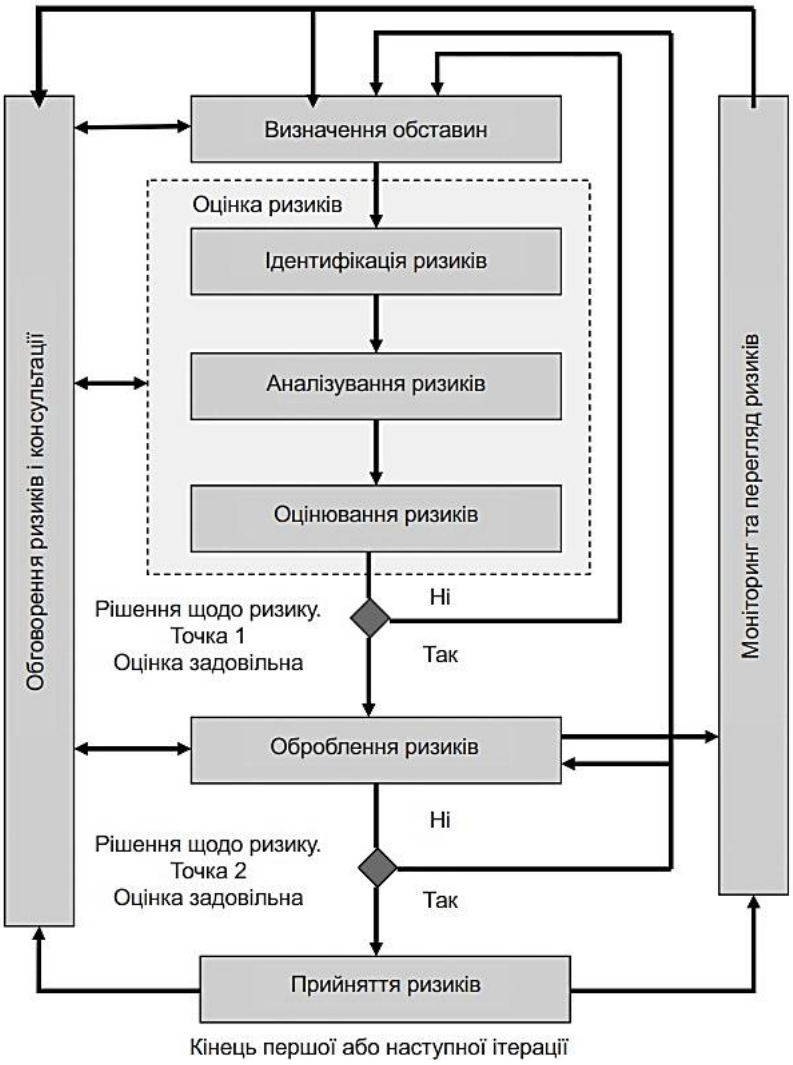

Рисунок 2.1 - Ілюстрація процесу управління ризиками ІБ за стандартом ISO 27005

На етапі визначення обставин визначаються зовнішні та внутрішні обставини для управління ризиками ІБ, що передбачає встановлення базових критеріїв, необхідних для управління ризиками інформаційної безпеки, визначення сфери застосування та її меж й забезпечення функціонування управління ризиками інформаційної безпеки прийнятого для організації.

Базові критерії:

- Критерії зіставлення ризиків;
- Критерії впливу;
- Критерії приймання ризиків.

Оцінка ризиків складається з таких дій:

- Ідентифікація ризику;
- Аналіз ризиків;
- Зіставлення ризиків.

Метою ідентифікації ризику є визначення того, що могло б статися, щоб спричинити потенційні втрати, і щоб отримати уявлення про те, як, де і чому ці втрати можуть виникати. Етапи, які входять в ідентифікацію ризику, повинні збирати вхідні дані для дії щодо аналізу ризику:

1. Ідентифікація активів СУІБ (активом є щось, що має цінність для організації і, отже, потребує захисту);
2. Ідентифікація загроз;
3. Ідентифікація існуючих засобів контролю;
4. Ідентифікація вразливостей;
5. Ідентифікація наслідків.

Методологія аналізу ризиків може бути якісною чи кількісною, або їх комбінацією залежно від обставин.

Рівні ризиків повинні порівнюватися з критеріями оцінювання ризику і критеріями прийняття ризику.

Для оцінювання ризиків підприємства виміряні ризики повинні порівнюватися з критеріями оцінювання ризику.

Для обробки ризику є чотири варіанти: модифікація ризику, прийняття ризику, усунення ризику і розподілення ризику.

2.1.2 NIST SP800-30

В NIST SP800-30 представлені підходи не тільки до оцінки ризиків, а й до організації діяльності з управління ризиками інформаційної безпеки на різних рівнях (від стратегічного до прикладного на рівні окремих інформаційних систем). На відміну від ISO 27005 даний документ містить більш розгорнуті описи кожного з елементів, а також рекомендації щодо застосування на практиці в різних ситуаціях.

Методика NIST SP800-30 передбачає попереднє оцінювання двох параметрів [2]: потенційного збитку і ймовірності реалізації загрози. Застосування системи управління ризиками безпосередньо пов’язано з можливістю підприємств виконувати свої основні функції в умовах постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків охоплює широке коло завдань, які пов’язані зі стратегією управління ризиками і є основою для розробки власної системи управління ризиками. Запропонований процес оцінювання ризику інформаційної безпеки, представляється у вигляді таблиці, яка відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий механізм отримання оцінок ризику істотно обмежує точність результатів.

Управління ризиком являє собою процес ідентифікації ризику, процес оцінки рівня ризику і процес здійснення заходів, спрямованих на зменшення ризику до прийнятного рівня.

Мета виконання процесів управління ризиком полягає в тому, щоб дати можливість підприємству виконати свою місію за рахунок:

1. Підвищення безпеки ІТ-систем, які зберігають, обробляють або передають інформацію в межах і поза організацією;
2. Підвищення інформованості та обізнаності керівництва щодо прийнятих рішень з управління ризиком для отримання обґрунтованих обсягів витрат, які повинні ставати невід'ємною частиною загального бюджету ІТ;
3. Надання допомоги керівництву в авторизації своїх ІТ-систем на основі результатів, що випливають з виконання процесів управління ризиком.

Управління ризиками є ітеративним процесом і його дії відбуваються на кожній стадії життєвого циклу розвитку ІТ-системи. Зменшення негативного впливу на організацію і потреба в нормальній базі для прийняття рішення становлять фундаментальні передумови для того, щоб організації здійснювали процес управління ризику для своїх ІТ-систем.

Використання такої методики передбачає наступні етапи:

- Опис характеристик системи;
- Ідентифікація загроз;
- Ідентифікація вразливостей;
- Аналіз наявних засобів захисту;
- Визначення значення ймовірності;
- Аналіз впливу;
- Визначення значення ризику;
- Вибір засобів захисту;
- Документування отриманих результатів.

Методологія оцінки ризику охоплює дев'ять головних кроків (Таблиця 2.1).

Таблиця 2.1 - Загальна схема оцінки ризику за NIST SP800-30

Вхід	Дії оцінки ризику	Результати
• Комп'ютерне обладнання • Програмне забезпечення • Системні інтерфейси • Дані та інформація • Люди	Крок 1. Характеристика системи	• Межі системи • Функції системи • Критичність системи і даних • Чутливість
• Історія атак на систему • Дані від розвідувальних агентств, NIPC, OIG, FedCIRC, ЗМІ	Крок 2. Ідентифікація загроз	• Формулювання загроз
• Звіти за попередніми оцінками ризиків • Результати аудитів • Вимоги до безпеки • Результати тестування безпеки	Крок 3. Ідентифікація вразливостей	• Перелік потенційних точок вразливостей
• Поточний стан контролю • Плановані заходи щодо контролю	Крок 4. Аналіз контролю	• Перелік поточних і планованих заходів щодо проведення контролю
• Мотивація джерел загроз • Ймовірність загроз • Природа уразливості • Поточний стан контролю	Крок 5. Визначення ймовірності	• Рейтинги ймовірності здійснення загроз
• Аналіз впливу на роботу • Оцінка критичності активів • Критичність даних • Чутливість даних	Крок 6. Аналіз впливу	• Рейтинги впливу загроз
• Ймовірність загрози для експлуатації • Розміри впливу • Адекватність планованих або поточних заходів з контролю	Крок 7. Визначення ризику	• Ризики і рівні допустимих ризиків
• Н/З	Крок 8. Рекомендації з контролю	• Рекомендовані заходи щодо контролю
• Н/З	Крок 9. Документальне оформлення результатів	• Звіт по оцінці ризиків

2.1.3 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика проведення оцінки ризиків в організації, що була розроблена інститутом Software Engineering Institute (SEI) при університеті Карнегі Меллон (Carnegie Mellon University).

Цей підхід був створений, щоб допомогти організаціям ідентифікувати і оцінити ризики інформаційних систем, поліпшити їх можливості і захистити себе від цих ризиків.

Особливість даної методики полягає в тому, що весь процес аналізу проводиться силами співробітників організації, без залучення зовнішніх консультантів. Для цього створюється спільна група, що включає як технічних фахівців, так і керівників різного рівня, що дозволяє всебічно оцінити наслідки для бізнесу можливих інцидентів в області безпеки і розробити контрзаходи.

OCTAVE передбачає наступні фази аналізу [3] (Рисунок 2.2):

1. Встановлення критеріїв оцінки ризику;
2. Розробка профілю загроз, пов’язаних з активом та місцями його зберігання;
3. Ідентифікація інфраструктурних вразливостей;
4. Розробка стратегії і планів безпеки.

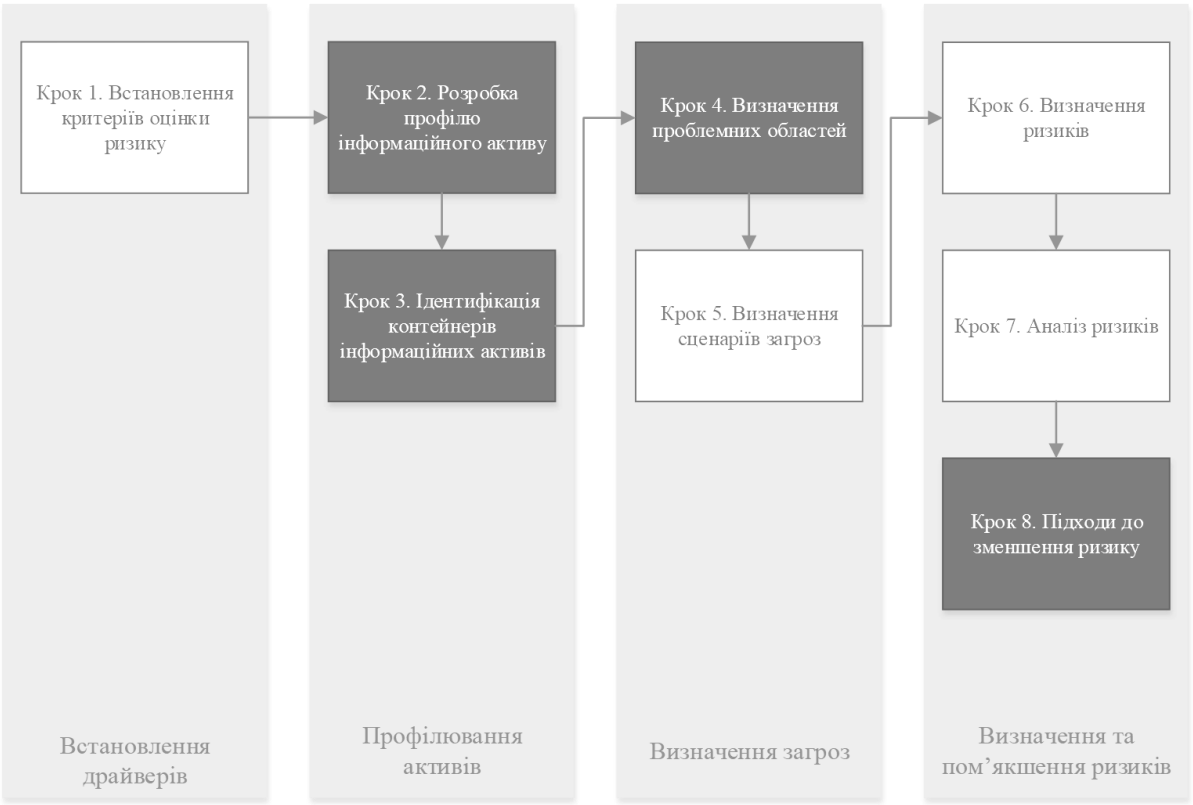

Рисунок 2.2 - Модель OCTAVE

Профіль загрози включає в себе актив, тип доступу до активу, джерело загрози, тип порушення або мотив, результат і посилання на опис загрози в загальнодоступних каталогах. За типом джерела, загрози в OCTAVE діляться на:

1. Загрози, які виходять від людини-порушника, який діє через мережу передачі даних;
2. Загрози, які виходять від людини-порушника, який використовує фізичний доступ;
3. Загрози, пов'язані зі збоями в роботі системи;
4. Інші.

Результатом може бути розкриття, модифікація, втрата або руйнування інформаційного ресурсу або розрив підключення, відмова в обслуговуванні.

Методика OCTAVE пропонує при описі профілю використовувати «дерево варіантів» (приклад подібного дерева для загроз типу 1 наведено на Рисунку 2.3). При створенні профілю загроз рекомендується уникати великої

кількості технічних деталей - це завдання другого етапу дослідження. Головне завдання першої стадії - стандартизованим чином описати поєднання загрози і ресурсу.

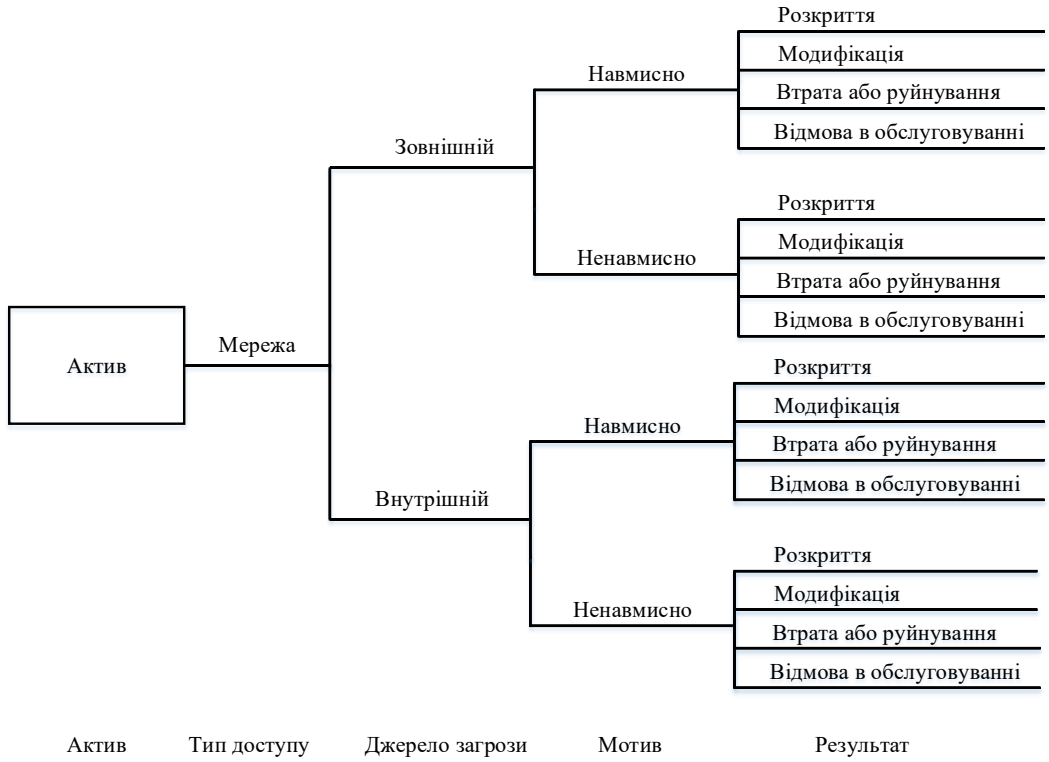

Рисунок 2.3 – Дерево варіантів, що використовується при описі профілю

Друга фаза дослідження системи відповідно до методики - ідентифікація інфраструктурних вразливостей. В ході цієї фази визначається інфраструктура, що підтримує існування активу (наприклад, якщо це база даних відділу кадрів, то для роботи з нею потрібен сервер, на якому розміщена БД, робоча станція співробітника відділу кадрів) і те оточення, яке може дозволити отримати до неї доступ (наприклад, відповідний сегмент локальної мережі). Розглядаються компоненти наступних класів: сервери; мережеве обладнання; СЗІ; персональні комп’ютери; домашні персональні комп’ютери користувачів, що працюють віддалено, але мають доступ до мережі

організації; мобільні комп’ютери; системи зберігання; бездротові пристрої; інше.

Група, яка проводить аналіз для кожного сегмента мережі, зазначає, які компоненти в ньому перевіряються на наявність вразливостей. Вразливості перевіряються сканерами безпеки на рівні операційної системи, мережевими сканерами безпеки, спеціалізованими сканерами (для конкретних web-серверів, СУБД та ін.), за допомогою списків вразливостей, тестових скриптів.

Для кожного компонента визначається:

- Список вразливостей, які треба усунути негайно;
- Список вразливостей, які треба усунути найближчим часом;
- Список вразливостей, щодо яких не потрібно негайних дій;

За результатами стадії готується звіт, в якому вказується, які вразливості виявлені, який вплив вони можуть надати на активи, які заходи треба вжити для усунення вразливостей.

Розробка стратегії і планів безпеки - третя стадія дослідження системи. Вона починається з оцінки ризиків, яка проводиться на основі звітів по двом попереднім етапам. У OCTAVE при оцінці ризику дається тільки оцінка очікуваного збитку, без оцінки ймовірності. Шкала: високий, середній, низький. Оцінюється фінансовий збиток, збиток для репутації компанії, життю та здоров’ю клієнтів і співробітників, збиток, який може викликати службове розслідування в результаті того чи іншого інциденту. Описуються значення, що відповідають кожній градації шкали (наприклад, для малого підприємства фінансовий збиток в $10000 – збиток високого рівня, для більшого - середнього).

Далі, розробляють плани зниження ризиків декількох типів:

- Довгострокові;
- На середню перспективу;
- Списки завдань на найближчий час.

Для визначення заходів протидії загрозам в методиці пропонуються каталоги засобів.

На відміну від інших методик, OCTAVE не передбачає залучення для дослідження безпеки ІС сторонніх експертів, а вся документація по OCTAVE загальнодоступна і безкоштовна, що робить методику особливо привабливою для підприємств з обмеженим бюджетом, виділеним на цілі забезпечення ІБ.

2.2 Порівняння методів оцінки ризиків

Таким чином, охарактеризувавши три найбільш поширені методики з управління ризиками в сфері інформаційної безпеки і здійснивши аналіз основних властивостей цих методик, стає можливим визначення відмінностей, основних переваг та недоліків методик ISO 27005, NIST SP800-30, OCTAVE (Таблиця 2.2).

Таблиця 2.2 – Порівняння методів оцінки ризиків

Методи оцінки ризиків	**Наявність перекладу української або російською мовою**	**Орієнтація на розмір підприємства**	**Наявність програмного інструментарію**	**Фази підходу**	**Тип оцінки ризику**	**Обробка ризиків**	**Необхідність в ресурсах**
ISO 27005	+	Можливе застосування для організацій різного розміру і галузей	+	• Визначення обставин • Ідентифікація ризику • Аналізування ризику • Оцінювання ризику • Оброблення ризику • Прийняття ризиків	Загальні настанови щодо якісної чи кількісної оцінки	• Модифікація • Прийняття • Усунення • Розподілення	Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження
NIST SP800-30	–	Застосовується для підприємств різного розміру. Розроблено, в першу чергу, для використання в федеральних організаціях США	+	• Характеристика системи • Ідентифікація загроз • Ідентифікація вразливостей • Аналіз контролю • Визначення ймовірності • Аналіз впливу • Визначення ризику • Рекомендації з контролю • Документальне оформлення	Змішана оцінка ризиків	• Прийняття • Запобігання • Обмеження • Планування • Дослідження і повідомлення • Перенесення	Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження
OCTAVE	–	Можливе застосування для організацій різного розміру і галузей	+	• Встановлення критеріїв оцінки ризику • Розробка профілю інформаційного активу • Ідентифікація контейнерів інформаційних активів • Визначення проблемних областей • Визначення сценаріїв загроз • Визначення ризиків • Аналіз ризиків • Підходи до зменшення ризику	Якісна оцінка ризиків	• Зниження • Прийняття	Власні ресурси організації, не експерти. Необхідне залучення співробітників як зі сторони IT, так і бізнесу

Висновки до розділу 2

Для побудови системи управління інформаційної безпекою, аналіз ризиків ІБ є одним з основних етапів, які повинні бути успішно виконаними. Саме тому вкрай важлива можливість впровадження швидкого і порівняно простого управління ризиками ІБ.

В даному розділі були проаналізовані відомі методології з аналізу ризиків, такі як ISO 27005, NIST SP800-30, OCTAVE. Був проведений порівняльний аналіз даних методологій, виявлено їх недоліки та переваги.

На основі проведеного аналізу, можна зробити висновок, що оптимальним варіантом для вибору методики управління ризиками інформаційної безпеки в контексті забезпечення безпеки інформації компанії та місцям її зберігання, обробки та передачі є адаптація та удосконалення відомих методик логічним об’єднанням їх переваг і мінімізацією недоліків.

3 ОСНОВНІ ПІДХОДИ ДЛЯ ОЦІНКИ ІНФОРМАЦІЙНОЇ ЦІННОСТІ

Майно або активи можна розділити на нематеріальну власність (знання, інформація, дані тощо) та матеріальне майно (обладнання та інші фізичні активи) (Рисунок 3.1).

Рисунок 3.1 – Співвідношення матеріальних та нематеріальних активів

Актуальна література явно уникає відповідати на питання про те, як оцінити інформаційну цінність. Вартість нематеріальних активів, які вважаються дуже важливими, регулярно ігнорується і, як правило, суб’єктивно оцінюється, що не є хорошою основою для прийняття рішень. Навіть сьогодні на цю тему написано мало робіт, адже важко знайти універсальний підхід для оцінки цінності активів.

Причиною труднощів в оцінці активів є те, що інформація, дані та знання не мають точно визначених значень, і їх вплив на результати бізнесу не зовсім зрозумілий. Проблеми виникають через те, що інформація не може бути визначена за допомогою речових доказів або розміру.

3.1 Вплив інформації на бізнес

Закон України «Про інформацію» дає наступне тлумачення поняття «інформації» - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Ділова інформація в бізнесі в основному служить основою для прийняття рішень, але вона також використовується для ведення та підтримки бізнес-процесів, полегшення спілкування між співробітниками і т. д.

На відміну від інших матеріальних активів, інформація в якості активу може мати різноманітні форми, бути дизайном продукту, технічними даними, інструкціями з управління, оперативними даними, знаннями співробітників, комп'ютерним програмним забезпеченням, робочими інструкціями, бізнес результатами і звітами, базою даних, системною документацією, керівництвом користувача, планами, засобами розробки та підтримки і т. д.

У бізнесі інформація є стратегічним ресурсом, який є ключовим для ведення бізнесу. Інформація є однією з найважливіших бізнес-цінностей, основним джерелом доходів і рушійною силою для створення нової цінності, для прийняття рішень, підвищення продуктивності, досягнення успіху на ринку і підтримки робочих процесів, засобом для комунікації. У кожному випадку інформація визначається як інструмент змін і інструмент формалізації та управління бізнес-середовищем.

Вплив, який спричиняє інформація, знання і дані зазвичай ідентифікується з фінансовими цінностями, але це тільки одна з форм впливу, який вона справляє на систему. Форми інформації, які можуть бути використані на ринку (наприклад, патенти, проекти, секретні контракти, плани і т. д.), можуть мати пряму фінансову цінність. Цінність цих форм інформації може бути кількісно виражена як частка можливої капіталізації на ринку. Пропорційно цьому розраховується ризик їх загрози. Разом з кількісним значенням інформація може мати інші значення, які не можуть бути виражені в фінансовому значенні. Така форма вартості якісна, яка може бути визначена залежно від умов її існування. Іншими словами, багато

аспектів, такі як працівники, які оброблятимуть інформацію, і умови, в яких працює бізнес-організація, визначають цінність інформації.

З 1980-х років при оцінці цінності інформації використовувалися три основні підходи [9]:

1. Якісний (на основі опису або ранжирування);
2. Кількісний (на основі чисельного розрахунку);
3. Їх комбінація.

Результати і ефективність оцінки цінності інформації залежать від вибору підходу. Хоча останнім часом інтерес до якісних підходів стає більш поширеним через акцент на оцінці нематеріальних активів, здається, що найбільш підходящий метод оцінки знаходиться десь між двома основними принципами. Зрештою, якісний підхід має кількісної складової, в результаті чого існуючі методи використовують кращі риси обох підходів.

Огляд характеристик двох основних підходів наведено в Таблиці 3.1.

Таблиця 3.1 - Форми і особливості оцінки вартості інформації

Форми інформаційного значення	**Зміст**	**Форма оцінки**	**Особливості оцінки**	**Цінність походить від**
Безпосередньо вимірний	Цінність може бути виражена у фінансовому значенні. Інформація купується або з'являється як продукт чиєїсь інтелектуальної роботи, яку можна оцінити з фінансової точки зору. Дуже часто інформація являє собою основу для виробництва нових знань, продуктів або послуг	Кількісна	- складні обчислення, часто незрозумілі, тривалі, вимагають програмної підтримки, нестандартної процедури; цінність визначена фінансово, хороша основа для аналізу витрат	Цінність може бути визначена з точки зору вартості створення, заміни або реконструкції

Продовження Таблиці 3.1

Форми інформаційного значення	**Зміст**	**Форма оцінки**	**Особливості оцінки**	**Цінність походить від**
Побічно вимірний	Інформаційна цінність в основному описується як якісна і суб'єктивна величина: вона сприяє більш успішному веденню бізнесу, і її важко оцінити з точки зору вартості.	Якісна	- простий, зрозумілий, суб'єктивний, не має відношення до фінансових витрат, не дає ніяких підстав для аналізу витрат / прибутку і визначення заходів безпеки	Цінність випливає з важливості для бізнес-процесів і функцій, важливості для людини і його роботи, важливості для бізнес-цілей

Кількісна оцінка підходить для визначення вартості активів, які мають пряму фінансову цінність у вигляді ліцензій, патентів, зразків і знань, куплених на ринку або зроблених відповідними учасниками. Їх фінансова вартість вказана при покупці або може бути визначена ціною виробництва. Важче визначити цінність інформації, що не є купленою на ринку або з'являється в ході бізнес-процесу. Якісна оцінка спрощує розуміння цінності інформації. В Таблиці 3.2 представлені метрики для кількісної та якісної оцінки цінності інформації.

Таблиця 3.2 – Метрики оцінки вартості інформації

Метрика	**Значення**
Фінансова вартість	• Виражає відношення вартість / прибуток в числах; • Використовує математичні та статистичні розрахунки • Може зробити оцінку більш важкою
Один, два, три, чотири, п'ять (1, 2, 3, 4, 5); ключова, критична, важлива, загальна, не важлива	• Метрика зрозуміла, повинна бути розроблена група правил для категоризації рівнів цінності • Успішність метрики залежить від суб'єктивності визначення критеріїв • Корисна, якщо фінансова вартість активів не важлива або невідома • Може застосовуватися до всіх елементів ризику • Не вимагає багато часу • Розрахунки прості • Аналіз витрат / прибутку не підтримується

3.2 Кількісна оцінка

Процедура кількісної оцінки пов’язана з оцінкою цінності інформації через її фінансову вартість. Є два методи оцінки. Перша, яка є фінансовою оцінкою, може використовуватися тільки для інформаційних активів, що характеризуються головним чином через вартість створення інформації (3.1):

$$V \approx F_{value}\ (value\ \approx financial) \tag{3.1}$$

де V – цінність інформації;

F_{value} – вартість інформації виражена в грошовому еквіваленті.

Якщо цінність інформації не може бути прямо виражена в грошовому еквіваленті, то оцінка є більш складною. В цьому випадку значення цінності може бути виражене у вигляді втрат / витрат, які з’являються у випадку відновлення або втрати інформації. Слід враховувати більше показників, таких як можливість припинення процесу або обслуговування, прибуток для інших суб’єктів і затримки, які з’являються через відсутність інформації (3.2).

$$V = \{\ \text{Значення для бізнесу}, \tag{3.2}$$
$$\text{Значення для конкурентів},$$
$$\text{Вартість відновлення активів},$$
$$\text{Вартість затримки процесів}\}$$

Кожен з перерахованих компонентів потім описується в фінансовому еквіваленті.

Результатом такої оцінки є фінансова цінність, яка визначає межі інвестицій в інформаційну безпеку.

3.3 Якісна оцінка

В процесі якісної оцінки можна використовувати різні форми графічних шкал, в яких зазначаються якісні (описові) значення цінності (важлива, середньої важливості, неважлива). Сама оцінка в основному заснована на досвіді оцінювача. Найбільшим недоліком цього підходу є нехтування фінансовою цінністю, а також висока суб'єктивність в оцінці.

Один із способів якісної оцінки - це «матриця цінностей». Він класифікує ділову інформацію в залежності від її важливості (стратегічна, тактична, оперативна і особиста інформація). Він також класифікує інформацію за віком (стара, середня або нова інформація). Процес оцінки включає в себе зв'язок інформації з двома аспектами оцінки. Отриманий результат відображається у вигляді матриці (Рисунок 3.2):

V - дуже цінна інформація;

M - середня цінна інформація;

L - менш цінна інформація.

Втрати - це третій вимір, але за рахунок збільшення кількості аспектів оцінки час оцінки також збільшується. Крім того, можна включити більшу кількість критеріїв оцінки, але не рекомендується використовувати більше семи.

	стара	середня	нова
стратегічна	L	V	V
тактична	L	M	V
оперативна	L	M	M
особиста	L	L	L

Рисунок 3.2 – Матриця співвідношення важливості інформації та її віку

Отже, як видно на Рисунку 3.2, стратегічна інформація, яка є новою, є дуже цінною. З іншого боку, більш стара інформація є менш цінною для бізнесу.

Висновки до розділу 3

В даному розділі робиться акцент на проблемі визначення інформаційної цінності та критеріїв, які використовуються для оцінки інформації. Оцінка цінності інформації вирішується шляхом перегляду ролі інформації в бізнесі. Для більш якісної оцінки важливо визначити критерії, які реально описують процеси в компанії, та за допомогою яких легко оцінити цінність інформації.

Існують два домінуючих метода оцінки та пов’язані з ними метрики: кількісний та якісний. Сама оцінка визначається обраною методологією і вона залежить від характеристик інформації, що оцінюється (чи можливо оцінити в грошовому еквіваленті чи ні). У кожному випадку обрана методологія та діапазон значень критеріїв повинні бути спрямовані на вибір найбільш ефективної оцінки і відповідно подальшого захисту інформації.

4 ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПІДПРИЄМСТВА РОЗДРІБНОЇ ТОРГІВЛІ

4.1 Особливості підприємств роздрібної торгівлі як об’єкта дослідження

Підприємства роздрібної торгівлі характеризуються наявністю великої кількості бізнес-процесів. Взаємозв’язок таких процесів є складним і потребує великої кількості автоматизованих систем для оперативного управління.

З іншої сторони наявність багатьох бізнес-процесів породжує велику кількість інформації та даних, необхідних для функціонування всього підприємства.

Такі підприємства характеризуються також великою кількістю співробітників, що в свою чергу призводить до необхідності контролю не тільки за безпекою процесів та інформаційних систем, але і зосередженні уваги на можливі ризики зі сторони співробітників, на навчанні співробітників з питань інформаційної безпеки, включаючи повідомлення про відповідальність за невиконання вимог інформаційної безпеки, розголошення конфіденційної інформації, отримання несанкціонованого доступу до конфіденційної інформації.

Всі ці особливості впливають на необхідність визначення, що захищати в першу чергу: яку інформацію, які інформаційні системи. Необхідним є впровадження зрозумілого ранжування цінної інформації, місць її зберігання та можливих ризиків.

Однією з основних проблем, яка стає явною на початкових етапах оцінки ризиків, це визначення яка інформація є цінною для підприємства. Керівники часто не мають уявлення про те, що може статися за відсутності інформації, в разі внесення несанкціонованих змін чи якщо інформація зникне. Деякі керівники суб’єктивно вважають, що вся інформація, яка створюється, обробляєтеся в їхньому підрозділі є не критичною, і вони не висувають вимоги щодо її захисту. Інші ж навпаки вважають всю інформацію критичною, що без неї зупиняться усі процеси і що захищати необхідно все. Суб’єктивна оцінка цінності інформації не є правильною та вигідною в даному випадку.

Для генеральних директорів важелем прийняття рішення є фактор вартості впровадження контрольних заходів по захисту інформації, для них вирішальними є гроші. Директор має зрозуміти вигоду від інвестицій у безпеку, адже підприємство може втратити набагато більше в разі виявлення інциденту інформаційної безпеки, який спричинив прямі фінансові втрати. Саме тому якісна оцінка цінності інформації та ризиків інформаційної безпеки не є вірним варіантом.

Підприємства роздрібної торгівлі постійно розвиваються. Цей розвиток починається з впровадження нових процесів, нових технологій та інших інновацій, що призводить до появи нових ризиків інформаційної безпеки. Саме тому підхід до управління ризиками має бути гнучким, щоб мати можливість повернутися до попереднього етапу, внести зміни та оновити результати оцінки ризиків, не витрачаючи на це великої кількості ресурсів (людських, часових, матеріальних).

Роздрібна торгівля є дуже конкуруючою сферою індустрії. Такі підприємства будь-якими засобами намагаються отримати перевагу на ринку, залучити на свою сторону більшу кількість клієнтів, отримувати найкращі партнерські пропозиції від постачальників. В роботі таких підприємств присутні і купівля цінної інформації про конкурентів, і переманювання співробітників. Підприємствам роздрібної торгівлі є необхідним мати уявлення про вектор атак зловмисників.

Важливим кроком до правильного впровадження процесу управління ризиками є узгодження ризик-апетиту підприємства. Ризик-апетит - рівень ризику, на який готова піти організація для досягнення бізнес-цілей; являє собою баланс між потенційними вигодами від виконання бізнес-діяльності і збитку, до якого дані дії можуть привести. Вибір релевантного підходу до оцінки ризиків сприятиме приведенню бізнес-діяльності до відповідності ризик-апетиту.

Управління ризиками інформаційної безпеки є основою до побудови системи управління інформаційною безпекою. Саме тому необхідним є визначення основних задач щодо впровадження процесу управління ризиками інформаційної безпеки для підприємств роздрібної торгівлі.

Основними завданнями процесу управління ризиками ІБ є наступні:

- Приведення у відповідність бізнес-діяльності підприємства і ризик-апетиту - завдяки визначенню та використанню рівня ризик-апетиту підприємства, більш точно оцінювати альтернативи ведення бізнесу і необхідних заходів для захисту інформації, відповідно, ставити адекватні цілі та розробляти механізми по управлінню ризиками;
- Поліпшення механізмів управління ризиками - вибір оптимального способу реагування на ризики ІБ на підставі всебічної інформації та чітко визначених критеріїв прийняття ризиків;
- Скорочення операційних витрат та інших втрат завдяки проактивному управлінню ризиками ІБ, шляхом їх ранньої ідентифікації та економічно-доцільної обробки;
- Визначення та управління множинними і пересічними ризиками ІБ - налагоджений процес з управління ризиками ІБ дозволить ефективніше управляти пов’язаними ризиками і формувати стратегію реагування на множинні ризики;
- Використання нових можливостей - шляхом визначення і аналізу різних подій і чинників, керівництво компанії зможе знизити витрати і вибрати оптимальні дії з управління ризиками ІБ.

4.2 Підхід до оцінки ризиків ІБ

Процес управління ризиками інформаційної безпеки складається з визначення підходів до проведення оцінки ризиків, оцінки ризику, обробки ризику, а також перегляду і вдосконалення процесу.

Рисунок 4.1 показує трьох етапний вигляд запропонованого підходу до управління ризиками інформаційної безпеки: мета запропонованого підходу полягає в тому, щоб зменшити ризики порушення безпеки, розуміння причин, які роблять інформаційні системи вразливими.

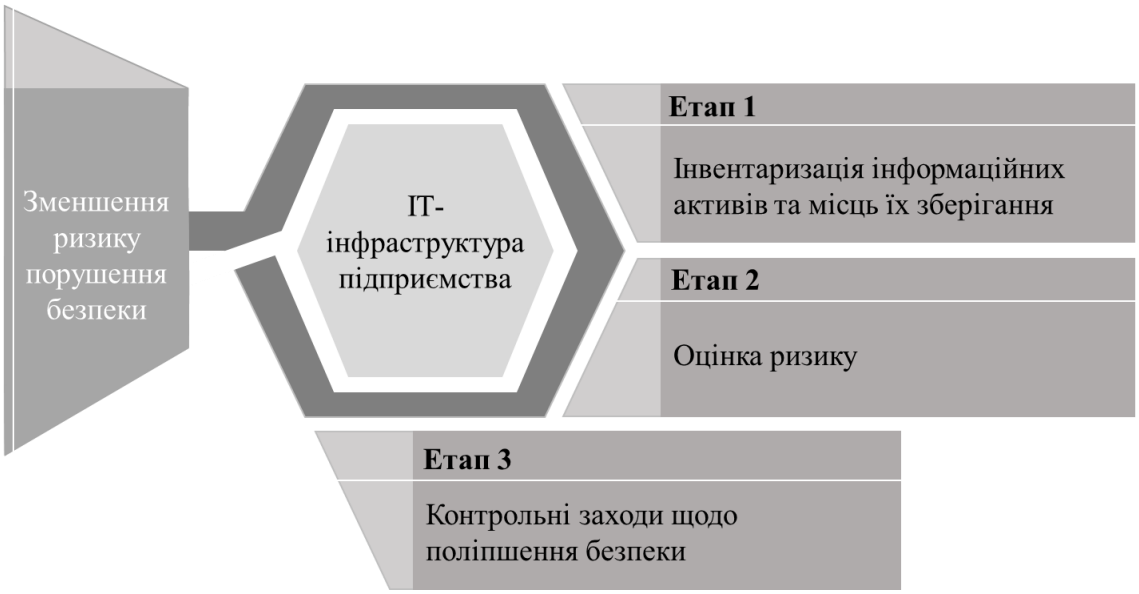

Рисунок 4.1 - Три етапи процесу управління ризиками інформаційної безпеки

Перший етап фокусується на збиранні інформації про те, яка інформація зберігається, обробляться, передається за допомогою певного місця зберігання (місцем зберігання в IT-інфраструктурі називається: персональні комп'ютери співробітників підприємства, сервери, мережеві папки, друковані документи, системи електронного документообороту та інші інформаційні системи, зовнішні місця зберігання і т.д.).

Наступна фаза полягає у визначенні слабких місць IT-інфраструктури підприємств роздрібної торгівлі, припускаючи постійні зміни та складні умови для підприємств даної індустрії, оцінці ризиків інформаційної безпеки для місць зберігання інформаційних активів підприємства. Друга фаза концентруються на розумінні того, які місця зберігання та активи мають найвищі ризики.

Третій етап полягає у створенні дієвого плану контрольних заходів по обробці ризиків.

Центральним елементом пропонованої моделі оцінки ризиків є оцінка IT-інфраструктури підприємства роздрібної торгівлі, створення рекурсивного механізму, який збирає дані про уразливість і загрози і виробляє рівень ризику, який можна виміряти і обробити.

Результати кожного етапу запропонованого підходу до оцінки ризиків представлені на Рисунку 4.2:

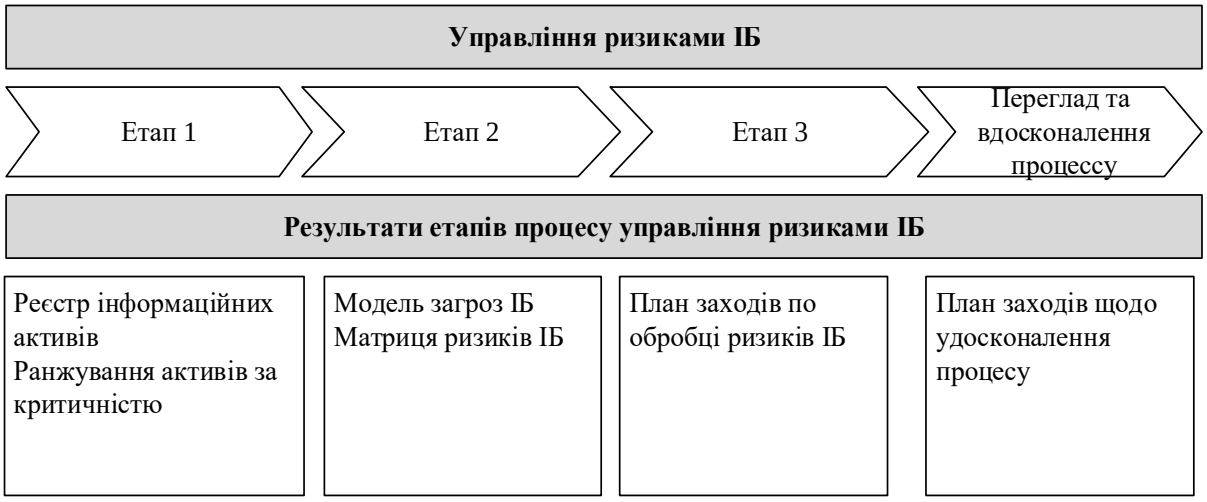

Рисунок 4.2 – Результати етапів процесу управління ризиками ІБ

Виконання етапів процесу управління ризиками ІБ нелінійне, і може виникнути необхідність повернення до попереднього етапу. Наприклад, при виконанні оцінки ризиків може виявитися, що обрані межі аналізу слід розширити, тому буде необхідно повернутися на етап 1.

4.3 Етап 1: Інвентаризація інформаційних активів та місць їх зберігання

Перед проведенням інвентаризації необхідно визначити межі виконання процесу оцінки ризиків ІБ. Пропонована модель визначає межами виконання оцінки ризиків ІБ межі дії системи управління ІБ (СУІБ). СУІБ - це комплекс організаційно-технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації підприємства:

- Конфіденційність - властивість інформації, що полягає в недоступності інформації або не розкриті її змісту неавторизованих особам, суб’єктам або процесам;
- Цілісність - властивість інформації, що полягає в забезпеченні її точності і повноти;

- Доступність - властивість інформації, що полягає в наявності інформації для користувача, коли це необхідно.

Межі СУІБ включають організаційні одиниці, бізнес-підрозділи, інформаційні системи та інші складові підприємства.

Інвентаризація інформаційних активів відбувається в порядку, зображеному на Рисунку 4.3.

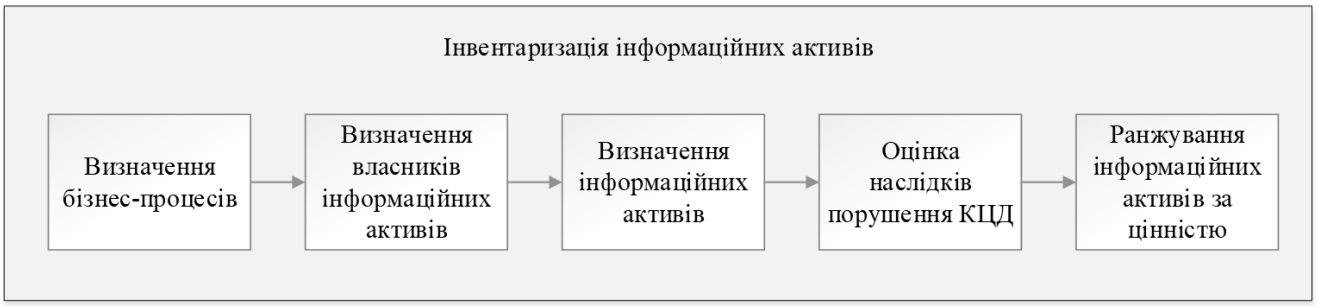

Рисунок 4.3 – Процес інвентаризації інформаційних активів

4.3.1 Визначення бізнес-процесів

Перед тим як ідентифікувати інформаційні активи, необхідно визначити бізнес-процеси організації, в рамках яких інформаційні активи створюються і використовуються.

Для підприємств роздрібної торгівлі бізнес-процеси можуть бути визначенні через служби організаційної структури підприємства, а саме:

- Служба управління ланцюгами поставок (логістика);
- Служба безпеки;
- Служба IT;
- Служба маркетингу;
- Юридична служба;
- Служба управління економікою та фінансами;
- Служба закупок;
- Аналітична служба;
- Служба нерухомості;

- Проектно-технологічна служба;
- Служба управління регіонами;
- Технічна служба;
- Служба управління персоналом.

4.3.2 Визначення власників інформаційних активів

Власники інформаційних активів - співробітники рівня керівників бізнес-напрямків, у яких є повноваження і відповідальність за захист важливої для бізнесу інформації.

Власники бізнес-процесів є власниками інформаційних активів, які створюються та / або використовуються в рамках їх напрямків діяльності. Власники бізнес-процесів мають необхідні знання, щоб визначити критичність активу, і повноваження, щоб організувати захист активу від порушення конфіденційності, цілісності та доступності. Обов’язки власника можуть бути делеговані, однак відповідальність повинна залишатися за призначеним власником активу.

4.3.3 Визначення інформаційних активів

Інформаційні активи – це будь-яка інформація, яка має цінність для підприємства і його бізнес-операцій.

Для визначення інформаційних активів необхідно провести інтерв’ю з власниками бізнес-процесів, в рамках яких визначити:

- Інформацію, яку створюють і обробляють підрозділи в електронному та паперовому вигляді;
- Місця, де інформація зберігається і обробляється, включаючи інформаційні системи, файлові сервера, локальні комп’ютери, паперові документи, зовнішні місця зберігання (наприклад, системи контрагентів або постачальників) і фізичні локації;

- Користувачів, які повинні мати доступ і працюють з інформацією всередині і поза компанією, із зазначенням організацій, підрозділів і посад;
- Критичність інформації для бізнесу, яка визначається за допомогою оцінки можливого збитку для підприємства в разі порушення конфіденційності, цілісності та доступності інформації.

Інформаційні активи в рамках області дії СУІБ повинні бути ідентифіковані та задокументовані і оцінені за рівнем збитку для підприємства в разі порушення їх конфіденційності, цілісності та доступності.

4.3.4 Оцінка наслідків порушення КЦД активів

Для кожного активу визначається також наслідки від реалізації ризиків порушення конфіденційності, цілісності, доступності (Таблиця 4.1).

Таблиця 4.1 – Наслідки при порушенні конфіденційності, цілісності та доступності активу

Рівень наслідків порушення КЦД	**Наслідки комерційним інтересам організації**	**Наслідки операційної діяльності**	**Наслідки відносинам з клієнтами і партнерами**	**Наслідки лояльності співробітників**
3	Комерційні інтереси або фінансове становище організації можуть бути істотно підірвані, втрата частки ринку	Критична втрата управлінського контролю, повна зупинка операційної діяльності, скасування поточних проектів	Серйозне погіршення іміджу організації, втрата довіри з боку значної частини клієнтів і партнерів, широка негативна популярність	Критичне зниження лояльності співробітників, масові звільнення

Продовження Таблиці 4.1

Рівень наслідків порушення КЦД	**Наслідки комерційним інтересам організації**	**Наслідки операційної діяльності**	**Наслідки відносинам з клієнтами і партнерами**	**Наслідки лояльності співробітників**
2	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 50 000 до 100 000 грн.	Середня втрата управлінського контролю, часткове зупинення операційної діяльності і труднощі в реалізації поточних проектів	Негативна інформація про підприємство поширюється в ЗМІ, втрата довіри з боку деякої частини клієнтів і партнерів	Значне зниження лояльності співробітників, погіршення клімату підприємстві і часті звільнення
1	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 10 до 50 000 грн.	Низька втрата управлінського контролю, незначні переривання операційної діяльності і незначні труднощі в реалізації поточних проектів	Втрата довіри деяких клієнтів або потенційних клієнтів, зниження довіри з боку деяких партнерів	Незначне зниження лояльності і скарги з боку співробітників
0	Порушення конфіденційності, цілісності та доступності інформації не має відчутних наслідків. Дана інформація документується в реєстрі інформаційних активів, але не бере участь в оцінці ризиків ІБ			

У даному підході для активу визначається рівень наслідків по кожному типу для кожної властивості інформації. Рівень наслідків порушення конфіденційності обчислюється за формулою (4.1).

$$L_{\text{cc}} = max\{C_c, C_o, C_{p\&c}, C_e\} \quad (4.1)$$

де L_{cc} – рівень наслідків від порушення конфіденційності активу;

C_c – рівень наслідків комерційним інтересам організації при порушенні конфіденційності;

C_o – рівень наслідків операційної діяльності при порушенні конфіденційності;

$C_{p\&c}$ – рівень наслідків відносинам з клієнтами і партнерами при порушенні конфіденційності;

C_e – рівень наслідків лояльності співробітників при порушенні конфіденційності.

Рівень наслідків порушення цілісності обчислюється за формулою (4.2).

$$L_{ci} = max\{C_c, C_o, C_{p\&c}, C_e\} \quad (4.2)$$

де L_{ci} – рівень наслідків від порушення цілісності активу;

C_c – рівень наслідків комерційним інтересам організації при порушенні цілісності;

C_o – рівень наслідків операційної діяльності при порушенні цілісності;

$C_{p\&c}$ – рівень наслідків відносинам з клієнтами і партнерами при порушенні цілісності;

C_e – рівень наслідків лояльності співробітників при порушенні цілісності.

Рівень наслідків порушення доступності обчислюється за формулою (4.3).

$$L_{ca} = max\{C_c, C_o, C_{p\&c}, C_e\} \quad (4.3)$$

де L_{ca} – рівень наслідків від порушення доступності активу;

C_c – рівень наслідків комерційним інтересам організації при порушенні доступності;

C_o – рівень наслідків операційної діяльності при порушенні доступності;

$C_{p\&c}$ – рівень наслідків відносинам з клієнтами і партнерами при порушенні доступності;

C_e – рівень наслідків лояльності співробітників при порушенні доступності.

4.3.5 Ранжування інформаційних активів за цінністю

В сучасному світі все більше зростає інтерес до нематеріальних активів. Сьогодні зростає їх вплив на успіх бізнесу, особливо в сфері ділової інформації.

Досить важко визначити цінність інформації, і тому зазвичай вона визначається суб’єктивно, що є проблематичним.

Оцінка і визначення вартості інформації є відкритою проблемою при визначенні розміру ризику інформаційної безпеки. Той факт, що деяка інформація є більш важливою або цікавою, мало що пояснює для керівника, якому необхідно інвестувати в безпеку. Оскільки інформаційна цінність повинна бути визначена більш точно, необхідно розуміти її вигляд, прояв, методи діяльності та структуру її цінності. Проблема виникає через необхідність в унікальному і зрозумілому методі оцінки, який також міг би підходити для процесу оцінки ризиків інформаційної безпеки.

У бізнес-системах інформація є стратегічним ресурсом, який є ключовим для ведення бізнесу. Інформація є однією з найважливіших бізнес-цінностей, основним джерелом доходів і рушійною силою для створення нової цінності.

При розгляді різних форм впливу інформації на бізнес необхідно враховувати такі особливості інформації:

1. Цінність інформації зростає з її використанням;
2. Цінність інформації нестабільна;
3. Інформаційна цінність зростає з власної точністю;
4. Інформаційна цінність зростає, коли вона комбінується з іншою інформацією;
5. Інформаційна цінність не зменшується з використанням.

Для оцінки значень інформаційної цінності, було встановлено, що інформація для підприємств роздрібної торгівлі оцінюється через її:

1. Значення комерційним інтересам підприємства;
2. Значення для операційної діяльності підприємства;
3. Значення для відносин з клієнтами і партнерами;
4. Значення для лояльності співробітників.

Для ранжування інформації за ступенем критичності необхідно по результатам оцінки наслідків від порушення конфіденційності, цілісності та доступності інформації визначити її цінність для організації.

У 3 розділі було зазначено, що існують різні підходи до оцінки цінності інформації. У даній роботі пропонується оцінювати цінність інформаційного активу за формулою 4.4.

$$V_{inf} = \frac{10}{N_C} \cdot (max\{C_{c.cia}\} + \max\{ C_{o.cia}\} + \max\{C_{p\&c.cia}\} + \max\{C_{e.cia}\}\}) \quad (4.4)$$

де V_{inf} – значення інформаційної цінності активу, $V_{inf} \in [\ 0{,}10\ ]$;

N_V – діапазон значень наслідків порушення КЦД, $N_{IV} \in [\ 0{,}12\ ]$;

$C_{c.cia}$ – рівень наслідків комерційним інтересам організації при порушенні конфіденційності, цілісності, доступності;

$C_{o.cia}$ – рівень наслідків операційної діяльності при порушенні конфіденційності, цілісності, доступності;

$C_{p\&c.cia}$ – рівень наслідків відносинам з клієнтами і партнерами при порушенні конфіденційності, цілісності, доступності;

$C_{e.cia}$ – рівень наслідків лояльності співробітників при порушенні конфіденційності, цілісності, доступності.

Для ранжування інформації необхідно використовувати запропоновану шкалу з Таблиці 4.2.

Таблиця 4.2 - Класифікація інформаційних активів за ступенем їх впливу на бізнес

Цінність інформації	**Рівень критичності інформації**
[8, 10]	К1 (особливо критична інформація)
[5, 8)	К2 (критична інформація)
[2, 5)	К3 (інформація середньої критичності)
< 2	К4 (некритична інформація)

В результаті інвентаризації, створюється реєстр з описом інформаційних активів, місць їх зберігання, а також допустимих користувачів активів у вигляді підрозділів і інших організаційних одиниць.

Інвентаризація інформаційних активів є безперервним процесом і повинна періодично переглядатися і доповнюватися власниками інформаційних активів. За фактом виявлення нового активу або зміни даних про існуючий, власник інформаційного активу повинен повідомити про це співробітників ІБ організації, які заносять необхідну інформацію в реєстр інформаційних активів. Після оновлення власник інформаційних активів повинен узгодити реєстр. Оновлений реєстр ініціює проведення додаткової оцінки ризиків за новими або оновленими інформаційними активами.

4.4 Етап 2: Оцінка ризиків ІБ

Ризик ІБ – рівень збитку, який понесе компанія, в разі реалізації загрози з використанням уразливості місця зберігання і обробки інформації компанії

На Рисунку 4.4 показаний процес для оцінки ризиків інформаційної безпеки.

Рисунок 4.4 – Процес оцінки ризиків інформаційної безпеки

Оцінка ризиків необхідна для визначення критичної для функціонування бізнесу інформації та збитків від порушення конфіденційності, цілісності та доступності цієї інформації.

4.4.1 Оцінка рівня схильності активів та місць їх зберігання та обробки до впливу ризику

Так як інформація зберігається і обробляється в певних місцях зберігання, саме які запропонований підхід пропонує захищати, тому необхідно оцінити з яким рівнем наслідків від порушення конфіденційності, цілісності та доступності активи зберігаються в даному місця зберігання.

Відповідно до рівнів наслідків порушення конфіденційності, цілісності та доступності активу, визначається рівень наслідків для місця зберігання.

Якщо загроза має вплив одразу на декілька властивостей інформації, то даний підхід пропонує визначати рівень наслідків порушення КЦД для місця зберігання активів за формулою (4.5)

$$L_{\text{c}} = max\{L_{\text{cc}}, L_{ci}, L_{ca}\} \quad (4.5)$$

де L_c – результуючий рівень наслідків порушення КЦД місця зберігання;

L_{cc} – рівень наслідків від порушення конфіденційності активів;

L_{ci} – рівень наслідків від порушення цілісності активів;

L_{cc} – рівень наслідків від порушення доступності активів.

Рівень схильності активів та місць їх зберігання та обробки до впливу ризику визначається за Таблицею 4.3.

Таблиця 4.3 – Залежність рівня схильності активів та місць їх зберігання та обробки до впливу ризику від рівня наслідків порушення КЦД

Рівень наслідків порушення КЦД	**Рівень схильності активів та місць їх зберігання та обробки до впливу ризику, %**
3	100
2	80
1	60
0	20

4.4.2 Ідентифікація вразливостей місць зберігання і обробки інформаційних активів

Визначення вразливостей місць зберігання і обробки інформаційних активів відбувається після створення і затвердження інвентаризаційного реєстру.

Для визначення вразливостей необхідно провести аудит налаштувань безпеки систем, обладнання, і контролів інформаційної безпеки, що діють в організації в наступних сферах, але не обмежуючись ними:

- Технічні засоби, програмне забезпечення, телекомунікаційне обладнання та підтримуюча інфраструктура:
  - Управління доступом;
  - Управління змінами;
  - Управління резервним копіюванням;
  - Управління задачами за розкладом;
  - Управління інцидентами;
  - Управління вразливостями.
- Процеси ІБ:
  - Управління мобільними пристроями;
  - Управління знімними носіями інформації;
  - Управління доступом;
  - Управління життєвим циклом інформаційних систем;
  - Моніторинг подій інформаційної безпеки;
  - Управління вразливостями;

- Управління інцидентами;
- Управління ризиками інформаційної безпеки;
- Криптографічний захист інформації;
- Захист від зловмисного коду;
- Управління резервним копіюванням;
- Контроль за установкою ПЗ на комп’ютерах користувачів;
- Безпека мережі;
- Управління сервісними організаціями.

- Кваліфікація і обізнаність персоналу, процедури адміністрування і механізми контролю процесів, розподіл ролей і відповідальності;
- Фізичне оточення і фізичні заходи захисту;
- Відповідність вимогам законодавства, договорів, стандартів і інших нормативних документів.

Для кожного процесу та для кожного місця зберігання складається перелік виявлених вразливостей.

Для кожної вразливості необхідно встановити її рівень. В запропонованому підході пропонуються наступні рівні вразливостей в існуючому середовищі:

- Високий рівень вразливості;
- Середній рівень вразливості;
- Низький рівень вразливості;

Рівень вразливості буде далі використаний в розділі 4.4.5 для оцінки ймовірності загрози

4.4.3 Ідентифікація загроз направлених на місця зберігання активів

На даному етапі необхідно розробити модель загроз ІБ. Модель загроз ІБ включає існуючі і потенційні типові загрози ІБ, які можуть бути спрямовані на порушення конфіденційності, цілісності та доступності інформації підприємства.

Для підприємств роздрібної торгівлі співвідношення типових загроз та основних властивостей інформації, на які вони впливають, наведений у Таблиці 4.4.

Таблиця 4.4 – Типи загроз

Група загрози	**Тип загрози**	**Основні властивості інформації, на які впливає загроза**		
Зовнішні атаки		К	Ц	Д
	Атаки, що викликають відмову в обслуговуванні			×
	Злом ключів	×		
	Злом паролів	×		
	Несанкціонована спроба доступу	×	×	×
	Модифікація мережевого трафіку		×	×
	Перехоплення повідомлень	×		
	Поширення комп’ютерних вірусів		×	×
	Поширення спаму			×
	Впровадження шкідливого коду	×	×	
	Впровадження троянських програм	×	×	
	Соціальна інженерія	×		
	Виконання зловмисного сканування	×		
	Злом веб сайтів		×	
	Підміна веб сайтів	×		
	Підміна облікових записів користувачів	×		
Навмисна некоректна експлуатація		К	Ц	Д
	Отримання несанкціонованого доступу до системи / мережі	×		
	Використання системи з метою порушення роботи			×
	Використання системи з метою шахрайства	×	×	
	Розкриття інформації, що використовується для входу в систему	×		
	Розкриття бізнес інформації	×		
	Завантаження або відправка неадекватного вмісту		×	×
	Зміна або додавання транзакцій, файлів або баз даних		×	×
	Зміна системних привілеїв без авторизації		×	×
	Зміна або установка ПО без авторизації		×	×
	Установка недозволеного ПО		×	×
Крадіжка		К	Ц	Д
	Крадіжка бізнес інформації	×		×
	Крадіжка комп’ютерного обладнання			×
	Крадіжка ПО	×		×
	Порушення авторських прав на програмне забезпечення		×	
	Крадіжка інформації для аутентифікації	×		
	Крадіжка інформації для ідентифікації особистості	×		

Продовження Таблиці 4.4

Група загрози	**Тип загрози**	**Основні властивості інформації, на які впливає загроза**		
Збої в роботі		К	Ц	Д
	Збій в роботі застосунків, розроблених всередині Компанії	×	×	×
	Збій в роботі застосунків, закуплених у сторонніх постачальників	×	×	×
	Збій в роботі системного ПО	×	×	×
	Збій в роботі комп'ютерного / мережевого обладнання		×	×
Порушення надання послуг		К	Ц	Д
	Пошкодження обчислювального центру, втрата обчислювальної техніки			×
	Пошкодження / втрата комунікаційних каналів / послуг			×
	Пошкодження / втрата допоміжного обладнання			×
	Втрата електроживлення			×
	Перевантаження системи			×
	Стихійні лиха			×
Ненавмисна неправильна експлуатація		К	Ц	Д
	Помилки користувачів		×	×
	Помилки адміністраторів / IT персоналу		×	×
Непередбачені наслідки змін		К	Ц	Д
	Непередбачені наслідки від зміни / впровадження нових бізнес-процесів	×	×	×
	Непередбачені наслідки від змін в ПЗ	×	×	×
	Непередбачені наслідки від змін в бізнес-інформації	×	×	×
	Непередбачені наслідки від змін в комп'ютерному / комунікаційному устаткуванні	×	×	×
	Непередбачені наслідки від змін в організації	×	×	×
	Непередбачені наслідки від змін в методах користувачів або засобах	×	×	×

Список загроз необхідно переглядати щорічно і додавати в нього інформацію, на підставі даних про інциденти ІБ, які трапилися на підприємстві або поза ним, і з використанням інших загальнодоступних джерел.

4.4.4 Аналіз існуючих контрольних заходів безпеки

Відсутність або неефективність контролів інформаційної безпеки представляють вразливість системи безпеки підприємства. Наявність і ефективність контролів інформаційної безпеки знижують ймовірність реалізації загрози, тому вони повинні бути описані в матриці ризиків і враховані при подальшій оцінці ймовірності реалізації загрози.

Контрольні заходи безпеки включають, але не обмежуються:

- Нормативну документацію, що описує процеси інформаційної безпеки:
  - Управління правами доступу інформаційних систем та мережевих ресурсів;
  - Управління засобами криптографічного захисту;
  - Управління змінами інформаційних систем та мережевих ресурсів;
  - Управління життєвим циклом інформаційних систем;
  - Управління інцидентами інформаційної безпеки;
  - Управління вразливостями;
  - Організація антивірусного захисту;
  - Стандарти безпечних налаштувань для операційних систем, баз даних та мережевого обладнання, що використовуються на підприємстві;
  - Моніторинг подій інформаційної безпеки;
  - Управління фізичною безпекою;
  - Управління мобільними та зовнішніми носіями інформації;
  - Управління резервним копіюванням даних інформаційних систем та мережевих ресурсів.
- Впровадження процесів інформаційної безпеки, описаних в нормативній документації;
- Розділення ролей та відповідальності в процесах інформаційної безпеки;

- Впровадження технічних заходів безпеки на серверах, персональних комп’ютерах співробітників, мережевому обладнанні та в приміщеннях підприємства;
- Проведення періодичних аудитів налаштувань безпеки для всіх рівнів інформаційної системи (ОС, БД, застосунок);
- Інформування та навчання співробітників підприємства та зовнішніх організацій з питань інформаційної безпеки;
- Впровадження програмного забезпечення для оперативного реагування на інциденти інформаційної безпеки (сканери, антивіруси, системи виявлення та запобігання вторгнень і т.п.).

4.4.5 Оцінка ймовірності та частоти реалізації загрози

Оцінка рівня загрози повинна враховувати рівень вразливостей, природу загроз і особливості, властиві різним типам загроз:

- Навмисні загрози - їх ймовірність залежить від мотивації, знань, компетенції та ресурсів, доступних потенційному зловмиснику, а також цінності активів, на які спрямовані загрози;
- Випадкові загрози - їх вірогідність може оцінюватися з використанням статистики і досвіду [10];
- Минулі інциденти, що показують уразливості, існуючі в системі безпеки організації;
- Нові розробки і тенденції з інформацією про реалізацію загроз, відомої із загальнодоступних джерел.

Імовірність виникнення загрози важко оцінювати у випадках, коли йдеться про навмисні дії людей (наприклад, несанкціонований доступ), тому що дії будуть залежати від існуючої системи захисту інформації на підприємстві. А давати оцінку виникнення навмисної загрози, не враховуючи систему захисту інформації, є невірним, так як зловмисник буде оцінювати свої сили, і якщо в погано захищеній організації він спробує зробити зловмисні дії, що призводять до збитку для

організації, то в добре захищеній організації, що здійснює пильний контроль дій співробітників, він не зважиться.

Розділимо зловмисників на категорії декількома способами, прийнявши за основу класифікації мету, доступ, ресурси, кваліфікацію і ризик.

Цілі зловмисників можуть бути різні: заподіяння шкоди, фінансова вигода, інформація і т. д. Цілі промислового шпигуна відрізняються від цілей синдикату організованої злочинності, і контрзаходи, які здатні зупинити першого, можуть навіть не потурбувати других. Розуміння цілей ймовірних зловмисників - це перший крок до з'ясування контрзаходів, які будуть ефективними.

Зловмисники мають різний рівень доступу: можливості члена будь-якої організації, наприклад, набагато більші, ніж будь-якого одинака. Зловмисники також сильно розрізняються за своїми фінансовими можливостями: деякі добре фінансуються, інші ні. Одні мають достатню технічну кваліфікацію, у інших її немає.

Різні класи зловмисників по-різному ставляться до ризику. Конкуренти, що втратили цінність на ринку, часто бувають згідні втратити все, аби потопити конкурента з собою. Злочинці миряться з ризиком опинитися у в'язниці, але, ймовірно, не захочуть мати неприємності понад ті, якими може обернутися реалізацію загрози підприємству. Ті, хто шукає слави зовсім не хочуть потрапити до в'язниці.

Зловмисник з практично необмеженим бюджетом найбільш гнучкий в рішеннях, так як він може використовувати свої кошти для різних цілей. Він може отримати доступ, підкупивши осіб, які мають доступ до потрібної інформації, і підвищити свій технічний рівень, купивши технологію або найнявши експертів (можливо, присвятивши їх в свої наміри, можливо, наймаючи їх під хибними приводами). Він може також використовувати гроші для зниження ризику, здійснюючи більш підготовлені і тому більш дорогі атаки.

Раціональний зловмисник (таких більшість) вибирає атаку, яка повністю покриє понесені витрати: кваліфікація, отримання доступу, трудові ресурси, час і ризик. Деякі атаки вимагають хорошої кваліфікації, але не вимагають ніякого

спеціального доступу: злом алгоритму кодування, наприклад. Кожен зловмисник намагається використовувати набір прийнятних для нього видів атак, відкинувши ті, які йому не підходять. Зловмисник вибере таку атаку, яка зменшує витрати і збільшує вигоди.

Тому ймовірність загрози вище 0 тоді, коли вигода від отриманої інформації перевищує витрати на її добування. Вона різко зростає при істотному збільшенні відношення ціни інформації до витрат на її добування – C_{inf} / C_g.

Рівень захищеності інформації визначає витрати на добування інформації. Його зростання зменшує відношення C_{inf} / C_g і, отже, ймовірність загрози.

Імовірність виникнення загрози залежить від багатьох факторів, основними з яких є:

- Ціна інформації, що захищається;
- Рівень інформаційної безпеки організації;
- Кваліфікація зловмисника, його ресурси та витрати на добування інформації;
- Криміногенна обстановка в організації (наявність співробітників, які будь не проти продати інформацію за хорошу винагороду).

У більшості випадків, якщо мова йде про навмисні дії людей, має місце їх матеріальна зацікавленість. Зловмисник буде здійснювати свої дії (атаки, НСД) на найменш захищені об’єкти, які і слід захищати.

Слід розглянути, чи є у даної організації джерело даної загрози, тобто вразливість. Якщо джерело загрози існує, то загроза може бути реалізована.

Підсумовуючи все вищесказане, даний підхід визначає наступні критерії оцінювання загрози, які наведені в Таблиці 4.6.

Таблиця 4.6 – Критерії оцінювання ймовірності реалізації загрози

Частота загрози та ймовірність	**Опис**	**Контролі і уразливості технічного характеру**	**Контролі і уразливості організаційного характеру**
Ймовірність реалізації загрози - низька. Очікувана частота реалізації загрози не перевищує 1 разу на 1-3 роки. Середньорічна частота реалізації загрози < 0,33.	Здатність реалізувати загрозу низька або джерело загрози недостатньо мотивоване. Діючі засоби захисту ускладнюють реалізацію загрози. Рівень вразливості низький. Відсутня статистика або інша інформація, яка б вказувала, що інцидент може статися. Використання вразливості можливо тільки при наявності прав адміністратора	- існують ефективні технічні засоби захисту, спрямовані на зниження рівня вразливості, однак регулярний контроль над роботою і ефективністю цих засобів не виконується - реалізація уразливості вимагає наявності у зловмисника високо-кваліфікованих навичок, спеціалізованих інструментів і додаткової інформації про місце розташування / передачі / носіїв інформаційних ресурсів (логіни користувачів, налаштування) - вразливість може бути використана тільки в комбінації з іншими вразливостями	- організаційні заходи (процедури, політики, мотиваційні та навчальні заходи) і / або засоби фізичного захисту, спрямовані на зниження рівня вразливості відповідають провідним практикам в області захисту інформації, однак контроль над дотриманням заходів захисту не виконується
Ймовірність реалізації загрози – середня. Очікувана частота реалізації загрози - приблизно 1 раз в 1-3 роки. Середньорічна частота реалізації загрози від 0,99 до 0,33	Джерело загрози мотивоване, існують передумови для реалізації загрози. Інформація про уразливість опублікована для широкої аудиторії, проте необхідні спеціальні технічні засоби для реалізації загрози. Використання вразливості можливо при наявності прав зареєстрованого користувача	- існуючі технічні засоби захисту, спрямовані на зниження рівня вразливості, неефективні, контроль над дотриманням заходів захисту не виконується - вразливість може бути використана тільки в комбінації з рядом інших вразливостей - вразливість може бути використана для отримання інформації про існуючих користувачів, деталі версій і налаштувань IT-систем (тобто інформації, яка може допомогти зловмисникові отримати НСД до інформаційних активів)	- вразливість може бути використана для отримання несанкціонованого фізичного доступу до інформаційних активів - організаційні заходи (процедури, політики, мотиваційні та навчальні заходи) і / або засоби фізичного захисту, спрямовані на зниження рівня вразливості, містять певні недоліки, контроль над дотриманням заходів захисту не виконується

Продовження Таблиці 4.6

Частота загрози та ймовірність	**Опис**	**Контролі і уразливості технічного характеру**	**Контролі і уразливості організаційного характеру**
Ймовірність реалізації загрози – висока. Очікувана частота реалізації загрози - один або декілька разів на рік. Середньорічна частота реалізації загрози ≥ 1	Джерелом загрози можуть бути співробітники компанії. Інформація про уразливість опублікована для широкої аудиторії. Існує статистика або інша інформація, яка вказує на те, що загроза скоріше за все здійсниться або можуть існувати серйозні причини або мотиви атакуючого, щоб здійснити такі дії	- технічні засоби захисту, спрямовані на зниження рівня вразливості, відсутні - вразливість легко використовувана для отримання прямого несанкціонованого доступу до інформаційних активів і / або отримання адміністративних привілеїв на рівні операційних систем / додатків	- організаційні заходи (процедури, політики, мотиваційні та навчальні заходи) і / або засоби фізичного захисту, спрямовані на зниження рівня вразливості, відсутні

4.4.6 Визначення рівня ризику ІБ

Для того щоб визначити рівень ризику необхідно порахувати величину збитку від реалізації загрози на місце зберігання та обробки інформаційних активів.

Існують різні підходи до оцінки величини збитків. У роботі пропонується оцінювати рівень фінансового збитку від ризиків порушення конфіденційності, цілісності та доступності інформаційного активу за формулою (4.6).

$$L_f = \sum_1^n \mathrm{C}_{inf} \cdot L_R \tag{4.6}$$

де L_f – фінансовий збиток від одноразової реалізації загрози, спрямованої на вразливість місця зберігання активу;

C_{inf} – вартість інформації, що зберігається в даному місці зберігання;

L_R – рівень схильності місця зберігання та обробки інформації до впливу ризику, $L_R \in [\,0{,}1\,]$.

Вартість інформації C_{inf} може формуватися на основі таких факторів, як:

- Чиста вартість інформаційного активу (вартість заміни або відновлення активу);
- Вартість утримання активу;
- Витрати в разі недоступності активу;
- Шкоди репутації організації;
- Зниження річного доходу;
- Зниження конкурентних переваг;
- Зниження ефективності внутрішніх процедур організації;
- Санкції за невідповідність законодавству.

Величина ризику від реалізації загрози протягом року обчислюється як добуток збитків від одноразової реалізації ризику на коефіцієнт, що характеризує середньорічну частоту появи загрози (4.7).

$$R = L_f \cdot F_e \tag{4.7}$$

де R – ризик від реалізації загрози, спрямованої на вразливість місця зберігання активу;

L_f – фінансовий збиток від одноразової реалізації загрози, спрямованої на вразливість місця зберігання активу;

F_e – середньорічна частота реалізації загрози.

В якості матеріальної величини для організації виберемо деякий поріг результатів діяльності організації. В запропонованому підході даний поріг оцінюється в розмірі 5% від чистого прибутку за рік, який ставиться у відповідність ризику інформаційних активів з високою значимістю для організації. Оцінки ризиків від втрати активів середньої і низької значущості будуть, відповідно, нижче порога матеріальності (Таблиця 4.7).

Таблиця 4.7 – Визначення шкали матеріальних збитків та відповідного рівня збитку

Матеріальна величина збитку	**Рівень ризику**
≥ 5% від чистого прибутку за рік	Високий
від 1% до 5% від чистого прибутку за рік	Середній
≤ 1% від чистого прибутку за рік	Низький

Підприємство приймає і не обробляє ризики з низьким рівнем. Середні ризики є потенційно прийнятними за погодженням з власниками інформаційних активів. Власники інформаційних активів - співробітники рівня керівників бізнес-напрямків, у яких є повноваження і відповідальність за захист важливої для бізнесу інформації. Власники визначаються на етапі інвентаризації інформаційних активів. Високі ризики вимагають негайної обробки.

4.5 Етап 3: Контрольні заходи щодо поліпшення безпеки

Для того щоб розробити контрольні заходи щодо поліпшення безпеки місць зберігання інформаційних активів підприємства слід провести обробку ризиків інформаційної безпеки.

Існують наступні загальні способи обробки ризиків ІБ:

- Прийняття ризику - залежить від можливих втрат від реалізації ризику і очікуваної частоти подій, а також політики організації в ставленні до діяльності, яка призводить до ризику, і простоти реалізації механізму контролю над ризиком;
- Зниження рівня ризику шляхом зменшення ймовірності впливу загрози або використання уразливості і / або зменшенням можливого збитку в разі здійснення ризику;
- Передача ризику третій стороні може бути обрана, якщо складно зменшити ризик до прийнятного рівня або його передача третій стороні більш виправдана з економічної точки зору;

- Уникнення ризику означає будь-які дії, при яких змінюються способи ведення бізнесу для того, щоб уникнути здійснення ризику. Уникнення ризику може включати відмову від певних бізнес-активностей, переміщення ресурсів із зони ризику, відмова від обробки цінної інформації або інші дії.

Способи обробки ризиків не є взаємовиключними. Наприклад, рівень ризику може бути знижений, а залишковий ризик застрахований. Також один спосіб обробки може покрити кілька ризиків ІБ.

Ефективність впровадження контрольних заходів можна оцінити за формулою 4.8.

$$E = \frac{R_{old} - R_{new}}{R_{old}} \quad (4.8)$$

де E – ефективність впровадження контрольних заходів з обробки ризиків інформаційної безпеки;

R_{old} – ризик без урахування контрольних заходів;

R_{new} - ризик з урахуванням контрольних заходів.

4.5.1 Зниження рівня ризиків ІБ

Співробітники ІБ підприємства розробляють заходи для зниження рівня ризиків ІБ. Для розробки заходів співробітники ІБ можуть залучати співробітників інших підрозділів підприємства, які відповідають за адміністрування місць зберігання і обробки інформаційних активів.

Заходи для зниження рівня ризику включають організаційно-технічні дії, спрямовані на зменшення ймовірності та шкоди реалізації загроз ІБ.

Під час розробки заходів необхідно визначити:

- Ризики, для яких будуть розроблені заходи;
- Дії, необхідні для зниження рівня ризиків;
- Очікувані результати за фактом виконання дій;
- Критерії успішного виконання дій;

- Необхідні ресурси на виконання заходів, включаючи людські, часові та фінансові ресурси;
- Остаточний рівень ризику після впровадження заходу.

Розроблені заходи повинні бути економічно-обґрунтованими, а саме необхідні ресурси не повинні перевищувати рівень збитку. При відсутності економічної доцільності зниження рівня ризику або якщо це зробити неможливо, повинні бути розглянуті варіанти передачі ризику третім сторонам або варіанти відмови від ризикових операцій або їх заміна на менш ризикові.

Рівень залишкового ризику не повинен перевищувати рівень ризик-апетиту підприємства, в іншому випадку, повинні бути розроблені додаткові заходи, які дозволять знизити рівень ризику до прийнятного.

Необхідно скласти план впровадження розроблених заходів. План повинен містити графік впровадження заходів, відповідальних за виконання заходів і терміни їх впровадження.

Для визначення пріоритету впровадження заходу використовується наступний підхід:

- Всі заходи поділяються на групи за рівнем ризику, для зниження якого вони призначені. Найвищий пріоритет присвоюється заходам, що знижує найвищий ризик;
- У кожній групі на перше місце ставляться ті заходи, які швидше і простіше реалізувати, і які дають найбільший ефект;
- Первинним заходам, від яких залежить успішність інших заходів, присвоюється більш високий пріоритет;
- Інші критерії, які можуть вплинути на пріоритетність заходів, наприклад, наявність ресурсів, законодавчі, фінансові, тимчасові та інші фактори.

4.5.2 Передача ризику ІБ

Рішення про передачу ризику третій стороні може бути прийнято, якщо даний спосіб є більш економічно-доцільним, ніж впровадження заходів щодо

зниження рівня ризику. Третьою стороною можуть бути страхова компанія або компанія, що забезпечує послуги з аутсорсингу потрібних процесів.

Кіберстрахування передбачає страхування бізнесу від втрат, пов'язаними з порушенням конфіденційності, цілісності та доступності (КЦД) інформації.

Кіберстрахування покриває:

- Витрати, що пов'язані з розголошенням конфіденційної інформації (крадіжка клієнтських або фінансових даних зловмисником), на проведення розслідування, оплату регуляторних штрафів, обробку цивільних позовів, інформування задіяних сторін;
- Витрати, пов'язані зі знищенням шкідливих програм і відновленням даних, які можуть виникнути через неавторизовані зміни або знищення даних (зміна формул розрахунку фінансової звітності співробітником підприємства);
- Витрати, пов'язані з відновленням інфраструктури та впровадженням засобів захисту, які можуть виникнути через порушення нормального функціонування інформаційної системи (не працює веб-сайт підприємства через зовнішньої атаки зловмисником).

Кіберстрахування включає не тільки випадки, пов'язані з хакерськими атаками, але і зупинку роботи інформаційних систем підприємства через:

- Природні катастрофи (землетруси, повені);
- Порушення фізичних приміщень та сервісів (збої в електриці, водопроводі);
- Інші типи збоїв в роботі організації, які призводять до порушення КЦД інформації.

4.5.3 Уникнення ризику ІБ

Рішення про припинення ведення певної бізнес-діяльності, яка може призвести до реалізації ризику ІБ, або її заміні на менш ризикову, має бути прийнято керівництвом підприємства. В даному випадку вигоди від виконання

бізнес-діяльності будуть істотно нижче, ніж можливі збитки від реалізації ризиків ІБ.

Уникнення ризику означає відмову від певних напрямків діяльності, переміщення ресурсів із зони ризику, відмова від обробки критичної інформації або інші дії.

4.5.4 Прийняття ризику ІБ

Керівництво підприємства може прийняти деякі ризики ІБ, вище рівня ризик-апетиту, якщо інші варіанти ризиків є неприйнятними або економічно-недоцільними.

4.6 Перегляд і вдосконалення процесу управління ризиками ІБ

Аналіз процесу управління ризиками інформаційної безпеки повинен проводиться на щорічній основі на предмет невідповідностей вимог даного підходу і провідним практикам у сфері ІБ. За результатами аналізу повинен бути складений план щодо поліпшення процесу управління ризиками ІБ, що включає дії по зміні підходів до процесу, критеріїв оцінки та прийняття ризиків.

За фактом впровадження плану поліпшення процесу управління ризиками може знадобитися підвищення кваліфікації співробітників ІБ та інших підрозділів підприємства. Для цього необхідно визначити і формально задокументувати необхідні компетенції співробітників і запланувати їх навчання.

4.7 Застосування підходу до аналізу ризиків інформаційної безпеки

4.7.1 Опис підприємства А як об’єкта для оцінки ризиків

Після визначення підходу до оцінки ризиків стало можливим оцінити ризики для підприємства А.

На сьогодні підприємство А налічує близько 40 тисяч співробітників та показник чистого прибутку за 2018 рік склав 2304 млн грн. Отже ризик-апетит для даного підприємства складає 115.2 млн грн.

Підприємство А входить в корпорацію, яка складається з 4 підприємств.

Організаційна структура даного підприємства складається з наступних підрозділів:

- Служба безпеки;
- Служби управління ланцюгами поставок;
- Служба інформаційних технологій;
- Служба розвитку роздрібної торгівлі;
- Автопарк;
- Юридична служба;
- Служба економіки і фінансів;
- Служба закупок;
- Відділ контролю якості продукції;
- Аналітичний відділ;
- Служба маркетингу;
- Служба управління персоналом;
- Проектно-технологічний відділ;
- Служба управління регіонами;
- Служба комерційної нерухомості;
- Технічна служба;
- Управління інформаційною безпекою підприємства.

Очолює підприємство генеральний директор - Головко Вячеслав Юрьевич.

Завданням підприємства є оцінка ризиків інформаційної безпеки для інформації, яка створюється, надходить, обробляється генеральним директором підприємства.

4.7.2 Етап 1: Інвентаризація інформаційних активів

Генеральний директор взаємодіє з усіма організаційними одиницями. Тому бізнес-процеси будуть включати всі служби підприємства, що були перечисленні вище.

Дані інвентаризації інформаційних активів були отримані в рамках проекту по місцю моєї роботи.

Результати інвентаризації інформаційних активів представлені в Додатку А в Таблиці А.1. Для кожного активу були визначені наслідки від реалізації ризиків порушення конфіденційності, цілісності, доступності. Результати даного кроку представлені в Додатку А Таблиці А.2.

Після того як визначені наслідки від порушення конфіденційності, цілісності, доступності активів визначимо цінність активів та проранжуємо їх від найбільш значущих до найменш. Результати наведені в Таблиці 4.8.

Таблиця 4.8 – Ранжування інформаційних активів за цінністю

№	Найменування ІА	Цінність інформації	Рівень критичності інформації
1	Стратегічні плани розвитку	8	К1 (особливо критична інформація)
2	Картка об'єкта	7	К2 (критична інформація)
3	Звіт про динаміку основних ключових показників підприємства	6	К2 (критична інформація)
4	Звіт про запланований бюджет в розрізі місяця, кварталу і року	6	К2 (критична інформація)
5	Звіт про прибутки і збитки Компанії в динаміці	6	К2 (критична інформація)
6	Аналітика продажів	6	К2 (критична інформація)
7	Звіт за основними ключовими показниками регіонів	6	К2 (критична інформація)
8	Комерційні умови роботи з постачальниками, тендерна документація	6	К2 (критична інформація)
9	Звіт про рентабельність магазинів	5	К2 (критична інформація)
10	Дані по нерухомості Компанії	5	К2 (критична інформація)
11	Концепція магазино-будування	5	К2 (критична інформація)
12	Картка проекту з даними по інноваціям, експериментам, покупкам нового обладнання	5	К2 (критична інформація)
13	Рішення ради директорів про покупку нового об'єкта	4	К3 (інформація середньої критичності)
14	Дані про виконання плану по товарообігу магазинами за минулий день	3	К3 (інформація середньої критичності)

Продовження Таблиці 4.8

№	Найменування ІА	Цінність інформації	Рівень критичності інформації
15	Звіт про дотримання плану по нормам запасів на розподільних центрах і магазинах	3	К3 (інформація середньої критичності)
16	Звіт про виконання плану товарообігу по акціях	3	К3 (інформація середньої критичності)
17	Дані по форс-мажорних ситуацій	3	К3 (інформація середньої критичності)
18	Звіт про плинність кадрів і некомплекту штату	3	К3 (інформація середньої критичності)
19	Звіт про втрати нормованих груп товарів	3	К3 (інформація середньої критичності)
20	Кадрові дані	3	К3 (інформація середньої критичності)
21	Звіти з продажу власної торгової марки	3	К3 (інформація середньої критичності)
22	Дані про відкриття нових магазинів	0	К4 (некритична інформація)

4.7.3 Етап 2: Оцінка ризиків ІБ

Оцінимо наскільки місця зберігання та обробки інформаційних активів схильні до впливу ризику. Результати наведені в Таблиці 4.9.

Таблиця 4.9 – Оцінка рівня схильності активів та місць їх зберігання та обробки до впливу ризику

Місце зберігання та обробки ІА	Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д	Рівень схильності активів та місць їх зберігання та обробки до впливу ризику порушення К, %	Рівень схильності активів та місць їх зберігання та обробки до впливу ризику порушення Ц, %	Рівень схильності активів та місць їх зберігання та обробки до впливу ризику порушення Д, %
ПК	3	2	2	100	80	80
Електронна пошта	3	3	3	100	100	100
Печатний документ	3	3	3	100	100	100
СЕД	3	3	3	100	100	100
Business Intelligence	3	2	2	100	80	80
Мобільний телефон	2	1	1	80	60	60

Наступним етапом є ідентифікація вразливостей та загроз, аналіз існуючих контрольних заходів та їх ефективності. Для отримання результатів було проведено інтерв'ю зі співробітниками ІБ підприємства, а також з адміністраторами місця зберігання. Був додатково проведений аудит налаштувань безпеки всіх інфраструктурних рівнів ІС (ОС, БД, застосунок).

На наступному етапі на основі аналізу існуючих контрольних заходів та вразливостей місць зберігання були визначені середньорічні частоти реалізації загроз. На основі цих даних були оцінені збитки від реалізації загроз та ризики.

Результати даного етапу наведені в Додатку А в Таблиці А.3.

Отже, в результаті оцінки ризиків інформаційних активів генерального директора та місць їх зберігання та обробки для підприємства А, були отримані результати, які представлені на Рисунку 4.5.

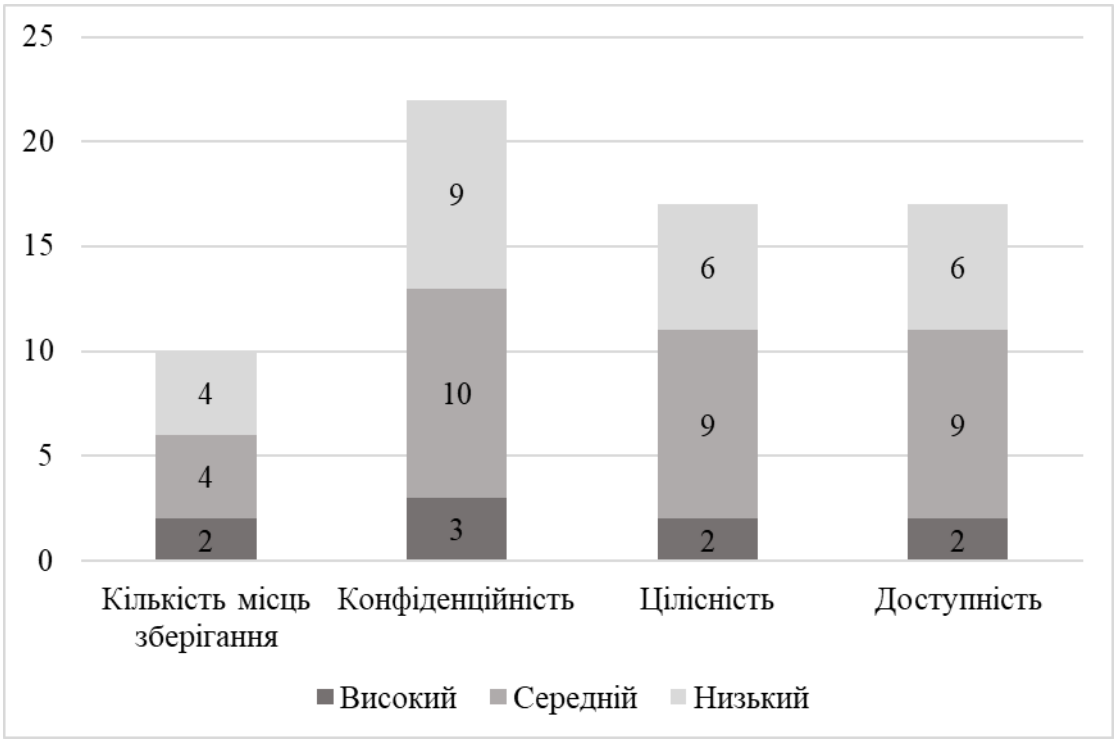

Рисунок 4.5 – Результати оцінки ризиків інформаційної безпеки для підприємства А роздрібної торгівлі

Високий рівень ризиків отримали наступні місця зберігання інформації:

- Персональний комп'ютер генерального директора;

- Система електронного документообігу.

На дані ризики слід звернути увагу в першу чергу, провести обробку ризиків та зменшити їх рівень до прийнятного – низького.

Середній рівень ризику мають місця зберігання:

- Персональний комп’ютер генерального директора;
- Система електронного документообігу;
- Електронна пошта;
- Паперові документи.

Основними причинами високого рівня ризиків є недостатня ефективність існуючих контрольних заходів, які б пом’якшували ризики.

21% вразливостей від їх загальної кількості пов’язані з відсутністю нормативних документів, що регламентують безпечну настройку окремих інфраструктурних компонентів аналізованих ІС.

79% вразливостей від їх загальної кількості пов’язані з

- Порушенням нормативних документів компанії:
  - Політика ІБ;
  - Процедура управління вразливостями;
  - Процедура управління правами доступу;
  - Процедура управління життєвим циклом ІС;
  - Стандарт безпечної настройки ОС Windows Server;
  - Стандарт безпечної настройки СУБД MS SQL.

4.7.4 Етап 3: Обробка ризиків ІБ

На етапі обробки ризиків в першу чергу слід приділити увагу ризикам с високим рівнем. На основі виявлених вразливостей та можливих загроз для ризиків с високим рівнем були розроблені рекомендації щодо пом’якшення ризиків (Додаток А Таблиця А.4).

Після проведення обробки ризиків наступними задачами є:

- Регулярна оцінка інформаційних ризиків (не рідше разу на рік або в разі істотних змін);
- У разі виявлення ризиків неприйнятного рівня - розробка плану щодо мінімізації ризиків;
- Впровадження плану заходів щодо мінімізації ризиків.

Висновки до розділу 4

В даному розділі був запропонований підхід до оцінки ризиків інформаційної безпеки. Даний підхід включає в себе особливості притаманні підприємствам роздрібної торгівлі. Кількісна оцінка ризику сприятиме приділенню уваги до більш критичних місць зберігання, обробки та передачі інформації компанії.

Розроблений підхід був застосований для підприємства А. Оцінка ризиків показала наявність 2 критичних місць зберігання інформаційних активів, які показали ризики високого рівня, які призводять до неприйнятних збитків (більше 5% від прибутку підприємства за рік). 4 місця зберігання показали середні рівні ризиків, які необхідно також обробляти після ризиків високого рівня.

В даному розділі для ризиків з високим рівнем були запропоновані рекомендації щодо їх зменшення, визначені необхідні фінансові інвестиції.

Запропонований підхід показав високу ефективність в умовах реального підприємства. Розроблений підхід може бути розширений та розвинутий, наприклад за рахунок додавання нових методів обробки ризику, оцінки цінності інформації. Проте зараз такий підхід може бути використаний підприємствами, які ставлять собі за ціль впровадити процес управління ризиками інформаційної безпеки.

ВИСНОВКИ

В даній роботі було проведене дослідження та аналіз можливих загроз і атак на підприємства роздрібної торгівлі. Аналіз показав, що дані підприємства щороку піддаються різноманітним атакам зі сторони як внутрішніх зловмисників, так і зі сторони зовнішніх. Частка останніх є набагато більшою, адже дані підприємства співпрацюють з багатьма постачальниками та підрядниками, можуть бути атаковані також зловмисниками зі сторони конкурентів. Проте найбільші збитки для підприємств роздрібної торгівлі приносять атаки, які були виконані внутрішніми зловмисниками. Найпоширенішими атаками для підприємств є впровадження шкідливого ПО, що свідчить про недостатню ефективність існуючої системи безпеки та недостатню обізнаність співробітників в сфері інформаційної безпеки.

Одним з важливих етапів побудови системи управління інформаційною безпекою є створення ефективного механізму управління ризиками, що дозволить приймати обґрунтовані рішення в даному напрямку. В роботі представлений огляд існуючих методів оцінки ризиків, які є поширеними на Україні. Детальне вивчення існуючих методів управління ризиками виявило необхідність побудови більш гнучкого та ефективного підходу до управління ризиками інформаційної безпеки підприємств роздрібної торгівлі, адже нинішні існуючі підходи мають ряд недоліків, такі як загальність викладу підходу, визначення ризиків якісними методами, необхідність значних ресурсів для впровадження .

Розроблений підхід для підприємств роздрібної торгівлі дозволяє кількісно оцінити ризики, класифікувати їх та своєчасно знизити високі ризики для підприємства, тим самим зменшити можливі збитки та зберегти кошти на відновлення в разі відмови або перебою в роботі місць зберігання та обробки інформації підприємства, а також виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки компанії. Підхід включає в себе особливості індустрії, які впливають на визначення впливу ризику на інформаційні активи (наслідки від дії ризику можуть впливати на комерційні інтереси, операційну

діяльність, відношення клієнтів та постачальників, лояльність співробітників), ранжування ризиків (високі ризики сприяють матеріальному збитку у розмірі більше ніж 5% від чистого прибутку підприємства за рік).

Запропонований підхід показав високу ефективність в умовах реального підприємства. В результаті використання даного підходу були оцінені можливі ризики для підприємства А, що належить до роздрібної торгівлі та отримані наступні результати:

1. Високий рівень ризиків отримали наступні місця зберігання інформації:
    - Персональний комп'ютер генерального директора;
    - Система електронного документообігу.
2. Середній рівень ризиків мають місця зберігання:
    - Персональний комп'ютер генерального директора;
    - Система електронного документообігу;
    - Електронна пошта;
    - Паперові документи.

Основними причинами високого рівня ризиків є недостатня ефективність існуючих контрольних заходів, які б пом'якшували ризики.

21% вразливостей від їх загальної кількості пов'язані з відсутністю нормативних документів, що регламентують безпечне налаштування окремих інфраструктурних компонентів аналізованих місць зберігання.

79% вразливостей від їх загальної кількості пов'язані з порушенням нормативних документів компанії.

Для ризиків з високим рівнем були запропоновані рекомендації щодо їх зменшення.

Таким чином, запропонувавши власний підхід до оцінки ризиків інформаційної безпеки, який враховує особливості індустрії роздрібної торгівлі, видає кількісний результат, визначає на які існуючі вразливості та недоліки контрольних заходів слід звернути увагу в першу чергу, дозволяє досягти підвищенню ефективності засобів захисту інформаційних систем підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.

2 Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology) [Текст]. – Gaithersburg: National Institute of Standards and Technology, 200.332. – 95 с.

3 Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст] / R. A.Caralli, J. F. Stevens, L. R. Young, L. R. Wilson.– Бостон: Університет Карнегі-Меллон, 2007. – 0.3354 с.

4 Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust [Електронний ресурс] // Symantec White Paper. – 200.335. – Режим доступу до ресурсу: https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf.

5 Cyber risk in retail: Protecting the retail business to secure tomorrow’s growth [Електронний ресурс]. – 200.337 – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/us-risk-200.337-retail-cyber-risk-report-04070.335.pdf

6 Информационная безопасность и розничная торговля [Електронний ресурс]. – 200.335 – Режим доступу до ресурса: https://www.cisco.com/c/ru_ru/about/press/press-releases/200.335/08-20.33d.html

7 Security trends in the retail industry [Електронний ресурс]. – 200.336 – Режим доступу до ресурса: https://www.ibm.com/downloads/cas/DO8MZRV9

8 Cyber security concerns in the retail sector [Електронний ресурс]. – 200.337 – Режим доступу до ресурса: https://www.grantthornton.ie/globalassets/0.33.-

member-firms/ireland/insights/factsheets/grant-thornton---cyber-security-concerns---retail.pdf

9 Скачек Л. М. ЦІННІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Текст] / Л. М. Скачек. // Інформаційна безпека. – 200.333. – №0.33(9). – С. 0.3352–0.3354.

10 Кибербезопасность: больше чем защита? [Текст] // Международное исследование EY в области информационной безопасности. – 2018. – С. 32.

Додаток А Результати оцінки ризиків підприємства А

Таблиця А.1 – Результати інвентаризації інформаційних активів та місць їх зберігання

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
1	Директор служби економіки та фінансів	Звіт про динаміку основних ключових показників підприємства	2.5	- Генеральний директор	Н/З	Н/З	- Генеральний директор - Директор служби економіки та фінансів	Н/З	Н/З
2	Директори всіх служб в рамках бюджету своєї служби	Звіт про запланований бюджет в розрізі місяця, кварталу і року	1.5	- Генеральний директор	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	Н/З	Н/З
3	Генеральний директор	Стратегічні плани розвитку	7.5	Н/З	- Генеральний директор - Рада директорів - Директори всіх служб	- Генеральний директор - Рада директорів - Директори всіх служб	- Генеральний директор - Рада директорів - Директори всіх служб	Н/З	Н/З
4	Директор служби розвитку роздрібної торгівлі	Картка об'єкта	4.25	Н/З	- Н/З	- Н/З	- Генеральний директор - Директор служби розвитку роздрібної торгівлі	Н/З	Н/З

Продовження Таблиці А.1

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
5	Генеральний директор	Рішення ради директорів про покупку нового об'єкта	5	Н/З	Н/З	Н/З	- Генеральний директор - Рада директорів	Н/З	Н/З
6	Генеральний директор	Звіт про прибутки і збитки Компанії в динаміці	6.25	Н/З	Н/З	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З
7	Директор аналітичної служба	Аналітика продажів	3.25	Н/З	Н/З	Н/З	- Генеральний директор - Директор служби економіки та фінансів - Директор аналітичної служби	- Директор аналітичної служба	Н/З
8	Директор аналітичної служба	Дані про виконання плану по товарообігу магазинами за минулий день	2.25	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок
9	Директор аналітичної служба	Звіт про дотримання плану по нормам запасів на розподільних центрах і магазинах	0.75	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок

Продовження Таблиці А.1

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
10	Директор аналітичної служба	Звіт про виконання плану товарообігу по акціях	1.25	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок
11	Директори всіх служб в рамках своєї служби	Дані по форс-мажорних ситуацій	0.5	Н/З	Н/З	Н/З	Н/З	Н/З	- Генеральний директор - Директор служб
12	Директор служби маркетингу	Дані про відкриття нових магазинів	0.002	- Генеральний директор	Н/З	Н/З	- Генеральний директор - Директор служби маркетингу	Н/З	Н/З
13	Директор аналітичної служба	Звіт про рентабельність магазинів	1.75	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служб економіки та фінансів	Н/З	Н/З	Н/З	Н/З
14	Директор служби управління регіонами	Звіт за основними ключовими показниками регіонів	1.25	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служби управління регіонами	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служби управління регіонами	Н/З	Н/З

Продовження Таблиці А.1

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
15	Директор служби управління персоналом	Звіт про плинність кадрів і некомплекту штату	0.25	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	Н/З
16	Директор аналітичної служба	Звіт про втрати нормованих груп товарів	0.5	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	Н/З
17	Директор служби комерційної нерухомості	Дані по нерухомості Компанії	0.25	Н/З	Н/З	Н/З	- Генеральний директор - Директор служби комерційної нерухомості	Н/З	Н/З
18	Генеральний директор	Концепція магазино-будування	0.75	- Генеральний директор	Н/З	- Підрядні організації	- Директори служб	Н/З	Н/З
19	Генеральний директор	Картка проекту з даними по плановним інноваціям, експериментам, покупкам нового обладнання	3.75	Н/З	- Генеральний директор - Директори всіх служб	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З
20	Директори всіх служб в рамках своєї служби	Комерційні умови роботи з постачальниками, тендерна документація	5	Н/З	Н/З	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З

Продовження Таблиці А.1

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
21	Директор служби управління регіонами	Кадрові дані	1.25	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	Н/З
22	Директор аналітичної служба	Звіти з продажу власної торгової марки	1.75	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	Н/З

Таблиця А.2 – Наслідки при порушенні конфіденційності, цілісності та доступності активу

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
1	Звіт про динаміку основних ключових показників підприємства	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
2	Звіт про запланований бюджет в розрізі місяця, кварталу і року	3	0	0	0	2	2	0	0	0	0	2	2	3	2	2

Продовження Таблиці А.2

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
3	Стратегічні плани розвитку	3	0	0	0	3	3	2	0	0	0	0	0	3	3	2
4	Картка об'єкта	3	0	0	0	3	2	0	2	2	0	0	0	3	3	2
5	Рішення ради директорів про покупку нового об'єкта	3	0	0	0	1	1	0	0	0	0	0	0	3	1	1
6	Звіт про прибутки і збитки Компанії в динаміці	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
7	Аналітика продажів	3	0	0	0	2	2	1	0	0	0	0	0	3	2	2
8	Дані про виконання плану по товарообігу магазинами за минулий день	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
9	Звіт про дотримання плану по нормам запасів на розподільних центрах і магазинах	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
10	Звіт про виконання плану товарообігу по акціях	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
11	Дані по форс-мажорних ситуацій	2	0	0	0	1	1	2	0	0	0	1	1	2	1	1
12	Дані про відкриття нових магазинів	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Звіт про рентабельність магазинів	2	0	0	0	2	2	0	0	0	0	0	0	2	2	2

Продовження Таблиці А.2

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
14	Звіт за основними ключовими показниками регіонів	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
15	Звіт про плинність кадрів і некомплекту штату	2	0	0	0	1	1	0	0	0	1	0	0	2	1	1
16	Звіт про втрати нормованих груп товарів	2	0	0	0	1	1	0	0	0	0	0	0	1	1	1
17	Дані по нерухомості Компанії	2	0	0	0	2	2	1	0	0	0	0	0	2	2	2
18	Концепція магазино-будування	2	0	0	0	2	2	0	0	0	0	0	0	2	2	2
19	Картка проекту з даними по плановим інноваціям, експериментам, покупкам нового обладнання	2	0	0	0	2	2	1	1	1	1	0	0	2	2	2
20	Комерційні умови роботи з постачальниками, тендерна документація	3	0	0	0	2	2	1	1	1	1	0	0	3	2	2
21	Кадрові дані	2	0	0	0	1	1	1	0	0	1	0	0	2	1	1
22	Звіти з продажу власної торгової марки	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1

Таблиця А.3 – Оцінки ризиків активів генерального директора підприємства та місць їх зберігання та обробки

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Крадіжка / втрата місць зберігання інформації (мобільних пристроїв, комп'ютерного обладнання і паперових документів)	×	×	×	ПК	Відсутність / недоліки процесу шифрування конфіденційної інформації на пристроях. Кінцеві користувачі відповідальні за шифрування інформації	Отримання несанкціонованого доступу до конфіденційної інформації компанії, в разі крадіжки ІТ-обладнання з конфіденційною інформацією, через відсутність / недоліків процесу та інструментів шифрування інформації	70.752	100%	0.99	70.04448
				Паперовий документ	Відсутність / недоліки відповідальності і контролю за фізичним захистом паперових документів при їх пересилці. У компанії не використовується одна кур'єрська служба для пересилки конфіденційних документів, з якої був би укладений договір і зафіксована відповідальність за фізичний захист документів при пересилці, в тому числі за нерозголошення конфіденційної інформації	Крадіжка паперових документів, на яких зберігається конфіденційна інформація, представниками кур'єрської служби або іншими зловмисниками, через відсутність контролю за пересиланням документів і відповідальності за фізичний захист документів при їх пересилці	9.75	100%	5	48.75
				Паперовий документ	Відсутність / недоліки політики чистого столу компанії при роботі з конфіденційною інформацією	Крадіжка паперових документів, на яких зберігається конфіденційна інформація, через відсутність / недоліків контролю за паперовими документами на робочих місцях співробітників	9.75	100%	3	29.25
				Мобільний телефон	Недоліки процесу і інструментів з управління мобільними пристроями (смартфони і планшети), за допомогою яких співробітники отримують доступ до конфіденційної інформації компанії. Відсутність політики щодо безпечного поводження з мобільними пристроями, налаштування безпеки пристроїв, контролю і моніторингу їх використання	Крадіжка / втрата мобільних пристроїв, через відсутність вимог до співробітників щодо безпечного поводження з мобільними пристроями, а також з-за недоліків процесу управління мобільними пристроями з боку компанії	4.75	80%	0.33	1.254

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Ненавмисне розкриття конфіденційної інформації співробітником компанії / представником зовнішньої організації	×			ПК	Відсутність / недоліки політики чистого екрану в приміщеннях компанії при роботі з конфіденційною інформацією на ІТ-обладнанні	Розголошення конфіденційної інформації зловмиснику, який отримав доступ до екрану мобільного пристрою, на якому відображається конфіденційна інформація	70.752	100%	3	212.256
				Електронна пошта	Відсутність контролю за відправкою листів по електронній пошті, що містять конфіденційну інформацію	Розголошення конфіденційної інформації при відправці електронного листа помилковому адресату	19.5	100%	0.99	19.305
Ненавмисне розкриття конфіденційної інформації співробітником компанії / представником зовнішньої організації	×			Паперовий документ	Відсутність процесу щодо безпечного використання, поширення та знищення інформаційних активів в паперовому вигляді. Немає обов'язкових вимог до маркування документів в залежності від їх рівня конфіденційності співробітниками компанії.	Розголошення конфіденційної інформації, через відсутність процесу безпечного поводження з конфіденційною інформацією, в тому числі маркування місця зберігання конфіденційної інформації	9.75	100%	0.99	9.6525
				Паперовий документ	Друк на мережевих принтерах не захищений паролем. Не виконується перевірка місць, де розташовані принтери, на предмет зберігання документів з конфіденційною інформацією і їх використання в якості чернеток	Розголошення конфіденційної інформації при отриманні доступу до паперового документу, який залишений без нагляду на принтері після друку або використовується в якості чернетки	9.75	100%	7	68.25
Умисне розкриття конфіденційної інформації співробітниками	×			Електронна пошта	Відсутність можливості контролювати відправку конфіденційної інформації по електронній пошті, якщо інформація була попередньо зашифрована засобами шифрування	Розголошення конфіденційної інформації, за допомогою її відправки по електронній пошті, через відсутність функціональності системи запобігання витоків інформації з аналізу зашифрованої інформації	19.5	100%	3	58.5
				Мобільні телефони	Відсутність / недоліки контролю за копіюванням інформації з ІС, в тому числі електронної пошти, на приватний пристрій. Відсутність формалізованого підходу до управління мобільними пристроями, а також вимог до співробітників щодо безпечного використання мобільних пристроїв	Розголошення конфіденційної інформації співробітниками, через відсутність контролю доступу користувачів і їх діями при роботі з конфіденційною інформацією компанії за допомогою особистих пристроїв	4.75	80%	5	19

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Непередбачені наслідки змін: впровадження нових бізнес-процесів, зміни в ПЗ, зміни в комп'ютерному / комунікаційному устаткуванні	×	×	×	ВІ	Недоліки в процесі управління змінами ІС, які можуть привести до неправомірного доступу до конфіденційної інформації. У компанії відсутній контроль за доступом розробників на продуктивне середовище, дотримання розробником вимог безпечної інсталяції та конфігурування застосунків	Розголошення конфіденційної інформації при отриманні несанкціонованого доступу до інформації в процесі розробки, тестування і установки змін ІС, через відсутність контролю доступу розробників на продуктивне середовище і відсутності стандарту безпечної інсталяції та конфігурування додатків	7.5	100%	0.99	7.425
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	ВІ	Відсутність / недоліки контролю доступу до інформаційних активів в хмарному середовищі, орендованій у хмарного провайдера, як внутрішніх користувачів, так і інших орендарів хмари і адміністраторів хмарних сервісів	Крадіжка конфіденційної інформації через недоліки в управлінні доступом до конфіденційної інформації компанії, яка зберігається і обробляється в хмарних сервісах	7.5	100%	0.33	2.475
				ПК	У компанії відсутня політика управління ліцензіями ПО, а також контроль за використанням неліцензійного ПЗ, яке може містити велику кількість вразливостей безпеки застосунків	Витік конфіденційної інформації, відмова в обслуговуванні ПК з використанням вразливостей неліцензійного ПЗ, встановленого на ІТ-обладнанні компанії, установка якого на ІТ-обладнання не контролюється	70.752	100%	0.99	70.04448
				Електронна пошта	Відсутність / недоліки контролю за масовими розсилками, визначенням і обробкою спам-листів, виявлення і видалення вірусного ПЗ в електронних листах	Крадіжка конфіденційної інформації, порушення працездатності ІС за допомогою шкідливого ПО або соціальної інженерії, що розсилаються по електронній пошті співробітникам компанії, з причини відсутності / недоліків засобів і механізмів контролю за масовими розсилками, визначенням і обробкою спам-листів, виявлення і видалення вірусного ПЗ в електронних листах	19.5	100%	0.99	19.305

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	Система електронного документо-обігу	Для адміністрування застосунку співробітниками СІТ застосовуються вбудовані облікові записи 'sa' і 'Administrator', які призначені для первинного розгортання ІС. Пароль до цих облікових записів відомий всім співробітникам зазначеного підрозділу. Згідно «Процедурі управління правами доступу» назви адміністративних облікових записів повинні однозначно ідентифікувати користувача, не даючи при цьому зайвої інформації про призначення облікового запису. Політика ІБ також встановлює вимогу, відповідно до якого будь-який доступ має здійснюватися із застосуванням персоналізованої облікового запису	Інформація про вбудовані облікові записи застосунків є загальнодоступною. Комбінація загальновідомих «логінів» і можливих варіантів пароля використовуються для реалізації атаки «brute force». Використання неперсоніфікованих адміністративних облікових записів, доступ до яких має велика кількість співробітників, істотно збільшує ризик компрометації таких облікових записів, а також ускладнює виявлення і розслідування пов'язаних з ними інцидентів ІБ	45.002	100%	0.99	44.55198
	×	×	×	Система електронного документо-обігу	Для окремих облікових записів застосунку застосовується внутрішня аутентифікація (наприклад, 'sa' і 'Administrator'). Для таких облікових записів на рівні програми не активований параметр «Застосовувати політику паролів», який приводить парольні налаштування програми у відповідність з парольними настройками на рівні ОС сервера БД. Поточні парольні настройки на рівні ОС не відповідають вимогам ІБ, які визначені в «Процедурі управління правами доступу», «Стандарті безпечної настройки операційних систем Windows Server»: Мінімальна довжина пароля - 7 символів. Рахунок не блокується після невдалих спроб входу в систему.	Використання слабких паролів або паролів, які легко визначити, в сукупності з відсутністю обмежень по числу вводів невірних паролів облікових записів істотно спрощують підбір паролів за допомогою застосування загальнодоступних утиліт («brute force»). У свою чергу, отримання зловмисником несанкціонованого доступу до застосунку може призвести до модифікації знищення і розкриттю критичних даних ІС, порушення її працездатності та інших несприятливих наслідків для Компанії	45.002	100%	0.99	44.55198

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	ПК	Неконтрольована установка ПО на стаціонарні робочі станції. Відсутність актуального білого списку ПО, яке може бути встановлено на робочі станції співробітників без узгодження співробітниками ІБ. Відсутність контролю того, що співробітники СІТ використовують файли ПО, перевірені та узгоджені співробітниками ІБ	Крадіжка або модифікація конфіденційної інформації, порушення працездатності ІС з використанням шкідливого ПО або ПО з уразливими безпеки, яке можна встановити на робочі станції без перевірки і узгодження співробітниками ІБ	70.752	100%	3	212.256
				ВІ	Використання ІС з вразливостями, уразливими конфігураціями, обліковими записами та паролями за замовчуванням. Відсутність формальної політики з управління вразливостями. У компанії відсутній процес за визначенням критичних оновлень ПО, в тому числі ОС, і процес їх швидкого встановлення на робочі станції і серверне обладнання. У компанії відсутній стандарт безпечної настройки ІС і мережевого устаткування, що включає список дозволених портів, протоколів, сервісів і необхідних заходів захисту для забезпечення безпечного функціонування. Відсутня процес по скануванню коду ПО на наявність вразливостей безпеки при установці оновлень	Крадіжка конфіденційної інформації з використанням вразливостей ІС і мережевого устаткування компанії, через відсутність процесу управління уразливими і стандартів безпечної настройки ІС і мережевого устаткування	7.5	100%	0.99	7.425
	×	×	×	ВІ	Відсутність / недоліки аутентифікації користувачів в корпоративну мережу, ІС на всіх інфраструктурних рівнях (ОС, СУБД, застосунок)	Крадіжка конфіденційної інформації, порушення працездатності ІС, доступ до якої був отриманий з використанням вразливостей механізму аутентифікації	7.5	100%	0.99	7.425
				ПК	Недоліки в роботі антивірусного захисту, в тому числі несвоєчасне оновлення сигнатурних баз, непроведення сканування комп'ютерів	Крадіжка або модифікація конфіденційної інформації, порушення працездатності ІС з використанням шкідливого ПО, установка і запуск якого не контролюється засобами антивірусного захисту через її відсутність, застарілої сигнатурної бази або можливості її відключення	70.752	100%	0.99	70.04448

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum C_{inf}$, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	Система електронного документо-обігу	Видача неузгоджених і / або некоректних прав доступу до ІС, недоліки механізму авторизації. Існуючі нормативні документи щодо процесу давно не актуалізувалися. Співробітники запитують права доступу виходячи із загального розуміння функціональності в системі. Матриці прав доступу не використовуються для видачі доступу в ІС. Права визначають відповідальні адміністратори на підставі свого досвіду або раніше наданих прав співробітникам. Відсутні формалізовані вимоги до проведення перевірок виданого доступу фахівцями ІБ.	Розголошення конфіденційної інформації при отриманні несанкціонованого доступу до інформаційних активів компанії, через недоліки процесу управління доступом	45.002	100%	3	135.006
				Система електронного документо-обігу	Недоліки процесу обмеження доступу до ІС при звільненні працівника. Доступ співробітників обмежується вручну фахівцем СІТ на підставі щоденного аналізу HR-системи, з метою визначити звільнених і переведених на нову посаду співробітників. Блокування доступу - відповідальність співробітників СІТ, у яких відсутні формалізовані вимоги до блокування даного доступу. Відсутня формалізований підхід до перевірки своєчасності блокування доступу співробітниками ІБ. Результати перевірок формально не документуються.	Розголошення конфіденційно інформації ї, порушення працездатності системи співробітниками, доступ яких до ІС не своєчасно заблокований	45.002	100%	0.99	44.55198

Таблиця А.4 – Рекомендації по впровадженню контрольних заходів для зменшення ризиків з високим рівнем

<table>
<tr><td>Контроль</td><td colspan="3">Впровадження процесу управління доступом до ІС</td></tr>
<tr><td>Рекомендації</td><td colspan="3">1. Розробити «Процедуру управління доступом до ІС», яка визначає вимоги до процесу надання, зміни і блокування доступу до інформаційних активів в ІС
2. Організаційно та технічно реалізувати доступ до ІС відповідно до вимог Процедури управління доступом
3. Впровадити вимоги процедури управління доступу до ІС, керуючись такими принципами:
• Мінімальної достатності прав доступу - користувач повинен мати доступ в системі мінімально необхідний для виконання службових обов'язків;
• Видача прав повинна базуватися на формальних вимогах, які визначають, які посади і відділи співробітників можуть запитувати які права по роботі з ІА в ІС, файлових сховищах або ІТ-сервісах. По можливості, створити матриці прав доступу в ІС, а в самих ІС реалізувати групи і / або ролі, за допомогою яких видавати доступ користувачам;
• "Чотирьох очей" (залучення декількох співробітників) для розмежування повноважень при здійсненні операцій з конфіденційною інформацією.
4. Впровадити вимоги до процесу аутентифікації користувачів в ІС:
• Вимоги до облікових записів користувачів:
o Кожному співробітнику повинен бути привласнений унікальний ідентифікатор в ІС;
o Всі системні і технічні облікові записи, які використовуються адміністраторами або іншими системами повинні бути визначені і формально задокументовані, а також визначені співробітники, які мають право використовувати дані облікові записи та / або відповідають за їх підтримку.
• Вимоги до парольних налаштувань:
o Паролі користувачів повинні бути унікальними для різних ІС або повинен використовуватися механізм однієї точки входу в усі системи;
o Паролі повинні відповідати заданим рівнем складності, змінюватися на періодичній основі, не повторюватися з раніше використовуваними (мінімум з 5 останніми);
o Блокування облікового запису користувача в разі 3-х невдалих спроб введення для звичайних користувачів і 5 спроб для адміністративних облікових записів (період блокування не менше 30 хв);
o Час неактивності користувача до блокування його робочого ПК повинна складати не менше 7 хвилин.
• Визначити вимоги до додаткових засобів аутентифікації користувачів. Для перевірки справжності користувача для доступу до високо-конфіденційної інформації повинні застосовуватися додаткові параметри: біометричні дані, смарт-карти співробітника
5. Провести повну перевірку прав доступу всіх співробітників компанії до ІА на предмет необхідності фактичного доступу користувачів. Після цього виконувати контроль коректності наданих прав доступу до ІА Компанії на періодичній основі, не рідше ніж раз у квартал.</td></tr>
<tr><td>Пріоритет</td><td>Високий</td><td>Складність</td><td>Середня</td></tr>
<tr><td>Тривалість</td><td colspan="3">2 місці</td></tr>
<tr><td>Фінансові інвестиції</td><td colspan="3">Впровадження рекомендацій не потребує фінансових інвестицій</td></tr>
</table>

Продовження Таблиці А.4

Контроль	**Впровадження політики чистого екрану в приміщеннях компанії при роботі з конфіденційною інформацією на ІТ-обладнанні**		
Рекомендації	1. Створити та забезпечити процедуру контролю за дотриманням правил «чистого стола та чистого екрана», яка буде включати (але не обмежуватися) наступними вимогами: • Документи і ІТ-обладнання, яке не використовується, слід прибирати з робочих столів і ховати в сейфи і інші шафи або приміщення, які обмежують доступ сторонніх осіб; • Вихід з систем або автоматичне блокування екрану ПК і ноутбука при закінченні роботи користувача; • Розміщення моніторів ПК і ноутбуків далеко від місць, де їх можуть побачити люди, у яких не повинно бути доступу до інформації (наприклад, далеко від вікон і прохідних ділянок приміщень). 2. Визначити та інформувати співробітників про дисциплінарні заходи, які можуть бути застосовані до співробітників компанії, в разі порушення прийнятих правил поводження з конфіденційною інформацією; 3. Співробітники ІБ повинні виконувати на періодичній основі контроль дотримання вимог процедури щодо безпечного поводження з конфіденційною інформацією; 4. Розробити Програму підвищення обізнаності в області ІБ, яка регламентує наступні аспекти: • Опис комплексної програми підвищення обізнаності співробітників та представників зовнішніх організацій, яка повинна включати (але не обмежуватися): o Зведену інформацію про існуючі нормативно-довідкові документи компанії в області ІБ, що регламентують захист конфіденційної інформації; o Порядок поводження з паперовими і електронними документами (зберігання / транспортування / знищення, політика чистого стола та чистого екрана); o Визначення відповідальності співробітників і представників зовнішніх організацій в разі недотримання вимог ІБ, в тому числі дисциплінарні заходи, які можуть бути застосовані до співробітників і представників зовнішніх організацій. 5. Впровадити Програму підвищення обізнаності персоналу та представників зовнішніх організацій в області ІБ: • Співробітники компанії, які в ході своєї робочої діяльності мають доступ до конфіденційної інформації, повинні щорічно проходити навчання в області ІБ, організоване працівниками ІБ.		
Пріоритет	Високий	**Складність**	Середня
Тривалість	3 місяці		
Фінансові інвестиції	30000-35000 $ Інвестиції складаються з: 1. 5000-10000 $ - створення силами підрядника онлайн порталу для розміщення матеріалів ІБ для вивчення співробітниками і оцінювання їх знань; 2. Від 25'000 $ - аутсорсинг створення і проведення тренінгів із загальних питань ІБ для 700 співробітників компанії, в розрахунку 1 тренінг триває до 3 год;		

Продовження Таблиці А.4

Контроль	**Впровадження процесу управління використовуваним ПЗ на обладнанні компанії**		
Рекомендації	1. Розробити та впровадити «Стандарт використання ПЗ на робочих станціях, серверному і мережевому обладнанні», включаючи наступне: • Створення та підтримка в актуальному стані списку стандартного ПЗ, дозволеного для установки на робочих ПК всіх співробітників; списку нестандартного ПЗ, яке можуть використовувати певні відділи і посади в рамках своєї роботи (наприклад, утиліти, які дозволено використовувати адміністраторам систем і користувачами з привілейованими правами для отримання доступу до баз даних); • Формалізувати вимоги заборони самостійної установки і зміни конфігурацій програмного забезпечення співробітниками (не з служби підтримки) на робочих ПК; • Формалізувати вимоги до перевірки безпеки ПЗ перед узгодженням установки ПЗ на робочі ПК / ноутбуки по заявці користувача; • Формалізувати розподіл ролей і обов'язків за впровадження і контроль установки і використання ПЗ на робочих станціях, серверному і мережевому обладнанні компанії; • Визначити та задокументувати дисциплінарні заходи, які застосовуються для співробітників, які встановили та використовували неузгоджене і / або заборонене ПЗ; • Формалізувати процес управління ліцензіями використовуваного ПЗ, включаючи контроль дотримання термінів і кількості ліцензій, а також заборона використання неліцензійного ПЗ; • Формалізувати процес управління оновленнями ПЗ, встановленого на робочих ПК; • Вести журнал аудиту змін ПЗ на робочих ПК, серверному і мережевому обладнанні; • Періодично перевіряти встановлене ПЗ на робочих ПК, серверному і мережевому обладнанні, і порівнювати його зі списком стандартних програм і зі затвердженими заявками співробітників на установку нестандартного ПЗ; документувати результати перевірки та усувати виявлені порушення. 2. Перевірити, що ніхто з користувачів не має прав на установку неавторизованого ПЗ на робочих ПК. Для цього необхідно перевірити, що забезпечено наступне: • Відсутність у користувача прав адміністратора на робочому ПК; • Обмеження доступу до виконуваних файлів недозволених для запуску і установки застосунків на рівні файлової системи; • Відсутність доступу користувача до мережевих ресурсів, на яких можуть зберігатися файли застосунків, невстановлених на робочому ПК; • Обмеження на використання зовнішніх носіїв інформації; • Обмеження доступу в мережу Інтернет.		
Пріоритет	Високий	**Складність**	Середня
Тривалість	2 місяці		
Фінансові інвестиції	Впровадження рекомендацій не потребує фінансових інвестицій		